THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface

About this Guide xli

CLI Command Sections xli

Supported Documents and Resources xlii

Related Common Documentation xliii

Related Product Documentation xliiv

Obtaining Documentation xlv

CHAPTER 1

Command Line Interface Overview 1

CLI Structure 2

CLI Command Modes 2

CLI Administrative Users 2

Administrative User Types 2

Authenticating Administrative Users with RADIUS 3

RADIUS SN-Admin-Permission / SN1-Admin-Permission AVP 3

RADIUS Mapping System 4

RADIUS Privileges 4

Authenticating Administrative Users with TACACS+ 4

Administrative User Privileges 5

Allowed Commands per User Type 6

Inspector Mode Commands 7

Operator Mode Commands 7

Administrator Mode Commands 9

Security Administrator Mode Commands 9

CLI Contexts 9

Understanding the CLI Command Prompt 10

CLI Command Syntax 11

Entering and Viewing CLI Commands 11
CHAPTER 2

AAA Server Group Configuration Mode Commands 23

description 25
diameter accounting 26
diameter authentication 30
diameter authentication failure-handling 34
diameter authentication failure-handling-template 36
diameter authentication strip-leading-digit 38
diameter dictionary 40
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>41</td>
</tr>
<tr>
<td>exit</td>
<td>42</td>
</tr>
<tr>
<td>radius</td>
<td>43</td>
</tr>
<tr>
<td>radius accounting</td>
<td>48</td>
</tr>
<tr>
<td>radius accounting apn-to-be-included</td>
<td>52</td>
</tr>
<tr>
<td>radius accounting algorithm</td>
<td>53</td>
</tr>
<tr>
<td>radius accounting billing-version</td>
<td>55</td>
</tr>
<tr>
<td>radius accounting gtp trigger-policy</td>
<td>56</td>
</tr>
<tr>
<td>radius accounting ha policy</td>
<td>58</td>
</tr>
<tr>
<td>radius accounting interim</td>
<td>60</td>
</tr>
<tr>
<td>radius accounting ip remote-address</td>
<td>62</td>
</tr>
<tr>
<td>radius accounting keepalive</td>
<td>64</td>
</tr>
<tr>
<td>radius accounting pdif trigger-policy</td>
<td>67</td>
</tr>
<tr>
<td>radius accounting rp</td>
<td>68</td>
</tr>
<tr>
<td>radius accounting server</td>
<td>71</td>
</tr>
<tr>
<td>radius algorithm</td>
<td>75</td>
</tr>
<tr>
<td>radius allow</td>
<td>76</td>
</tr>
<tr>
<td>radius attribute</td>
<td>78</td>
</tr>
<tr>
<td>radius authenticate</td>
<td>84</td>
</tr>
<tr>
<td>radius authenticator-validation</td>
<td>86</td>
</tr>
<tr>
<td>radius charging</td>
<td>87</td>
</tr>
<tr>
<td>radius charging accounting algorithm</td>
<td>90</td>
</tr>
<tr>
<td>radius charging accounting server</td>
<td>92</td>
</tr>
<tr>
<td>radius charging algorithm</td>
<td>95</td>
</tr>
<tr>
<td>radius charging server</td>
<td>96</td>
</tr>
<tr>
<td>radius ip vrf</td>
<td>99</td>
</tr>
<tr>
<td>radius keepalive</td>
<td>101</td>
</tr>
<tr>
<td>radius mediation-device</td>
<td>104</td>
</tr>
<tr>
<td>radius probe-interval</td>
<td>105</td>
</tr>
<tr>
<td>radius probe-max-retries</td>
<td>106</td>
</tr>
<tr>
<td>radius probe-timeout</td>
<td>107</td>
</tr>
<tr>
<td>radius server</td>
<td>108</td>
</tr>
<tr>
<td>radius trigger</td>
<td>112</td>
</tr>
</tbody>
</table>
CHAPTER 4

Accounting Policy Configuration Mode Commands

- accounting-event-trigger
- accounting-keys
- accounting-level
- accounting-mode
- apn-name-to-be-included
- attribute
- cc
- end
- exit
- max-containers
- operator-string
- rf
- service-context-id
- session
- trigger-type

CHAPTER 5

ACL Configuration Mode Commands

- deny/permit (by source IP address masking)
- deny/permit (any)
- deny/permit (by host IP address)
- deny/permit (by source ICMP packets)
- deny/permit (by IP packets)
- deny/permit (by TCP/UDP packets)
- description
- end
- exit
- readdress server
- redirect context (by IP address masking)
- redirect context (any)
redirect context (by host IP address) 188
redirect context (by source ICMP packets) 190
redirect context (by IP packets) 194
redirect context (by TCP/UDP packets) 198
redirect css delivery-sequence 203
redirect css service (any) 204
redirect css service (by host IP address) 207
redirect css service (by ICMP packets) 210
redirect css service (by IP packets) 214
redirect css service (by source IP address masking) 218
redirect css service (by TCP/UDP packets) 221
redirect css service (for downlink, any) 226
redirect css service (for downlink, by host IP address) 229
redirect css service (for downlink, by ICMP packets) 232
redirect css service (for downlink, by IP packets) 236
redirect css service (for downlink, by source IP address masking) 240
redirect css service (for downlink, by TCP/UDP packets) 243
redirect css service (for uplink, any) 248
redirect css service (for uplink, by host IP address) 251
redirect css service (for uplink, by ICMP packets) 254
redirect css service (for uplink, by IP packets) 258
redirect css service (for uplink, by source IP address masking) 262
redirect css service (for uplink, by TCP/UDP packets) 264
redirect nexthop (by IP address masking) 269
redirect nexthop (any) 272
redirect nexthop (by host IP address) 275
redirect nexthop (by source ICMP packets) 278
redirect nexthop (by IP packets) 282
redirect nexthop (by TCP/UDP packets) 286

CHAPTER 6

ACS Bandwidth Policy Configuration Mode Commands 291
end 292
exit 293
flow limit-for-bandwidth 294
group-id 295
ACS Charging Action Configuration Mode Commands 297

allocation-retention-priority 299
billing-action 301
cca charging credit 304
charge-units 306
charge-volume 308
content-filtering processing server-group 311
content-id 312
deactivate-predefined-rule 314
end 315
exit 316
flow action 317
flow idle-timeout 324
flow limit-for-bandwidth 326
flow limit-for-flow-type 329
ip tos 331
ip vlan 333
nexthop-forwarding-address 335
pco-custom1 336
product-offer-id-avp 337
qos-class-identifier 338
qos-renegotiate 339
retransmissions-counted 341
service-detection 342
service-identifier 344
stripurl token 345
tft packet-filter 347
tft-notify-ue 348
throttle-suppress 349
tos 350
tpo profile 352
video bitrate 353
video cae-readdressing 355
video detailed-statistics 357
video optimization-preprocessing all 359
video optimization-preprocessing cae-readdressing 360
video pacing by-policing 361
xheader-insert 363

CHAPTER 8

ACS Configuration Mode Commands 365
accelerate-flow 369
access-ruledef 370
bandwidth-policy 372
buffering-limit 374
charging-action 376
check-point accounting 378
content-filtering category match-method 380
content-filtering category policy-id 381
credit-control 383
diameter credit-control 385
drdr-format 386
drdr-ipproto-port-map 388
drdr-udr-flow-control 389
end 390
exit 391
fair-usage deact-margin 392
fair-usage tcp-proxy 394
fair-usage threshold-percent 396
firewall dos-protection flooding 398
firewall dos-protection ip-sweep 400
firewall flooding 402
firewall flow-recovery 403
firewall icmp-destination-unreachable-message-threshold 405
firewall license 406
firewall max-ip-packet-size 407
firewall mime-flood 408
firewall nat-alg 409
firewall no-ruledef-matches 411
firewall port-scan 412
firewall protect-servers  414
firewall ruledef  416
firewall tcp-syn-flood-intercept  418
firewall track-list  419
fw-and-nat action  421
fw-and-nat policy  423
group-of-objects  425
group-of-prefixed-urls  427
group-of-ruledefs  429
h323 time-to-live  431
h323 timeout  432
h323 tpkt  434
h323 version  435
host-pool  436
idle-timeout  438
imsi-pool  440
ip dns-learnt-entries  442
ip max-fragments  444
label content-id  445
nat allocation-failure  446
nat allocation-in-progress  447
nat ip downlink reassembly-timeout  449
nat tcp-2msl-timeout  450
nat unsolicited-pkts  451
p2p-ads-group  453
p2p-detection attribute  455
p2p-detection behavioral  457
p2p-detection ecs-analysis  459
p2p-detection protocol  461
packet-filter  483
passive-mode  485
pep-service  486
policy-control bearer-bw-limit  488
policy-control bind-default-bearer  489
policy-control burst-size  491
policy-control charging-action-override 492
policy-control charging-rule-base-name 493
policy-control dynamic-rule-limit 495
policy-control l7-dynamic-rules 496
policy-control retransmissions-counted 498
policy-control update-default-bearer 499
port-map 501
qos-group-of-ruledefs 503
radio-congestion 505
readdress-server-list 507
redirect user-agent 509
rulebase 510
rulebase-list 512
ruledef 514
service-scheme 516
sip advanced 518
statistics-collection 519
subs-class 521
subscriber-base 522
system-limit l4-flows 523
tethering-database 525
tethering-detection 527
timedef 528
tpo policy 530
tpo profile 531
trigger-action 532
trigger-condition 534
udr-format 536
url-blacklisting match-method 538
xheader-format 540

CHAPTER 9 ACS Group-of-Objects Configuration Mode Commands 543
doc 544
exit 545
member-object 546
CHAPTER 16
ACS QoS-Group-of-Ruledefs Configuration Mode Commands
add-group-of-ruledef 586
add-ruledef 587
end 588
exit 589

CHAPTER 17
ACS Readdress Server List Configuration Mode
consecutive-failures 592
end 594
exit 595
reactivation-time 596
response-timeout 598
server 600

CHAPTER 18
ACS Rulebase Configuration Mode Commands
action priority 607
active-charging rf 611
bandwidth default-policy 613
billing-records 614
cca diameter requested-service-unit 616
cca quota 618
cca quota time-duration algorithm 620
cca radius accounting interval 622
cca radius charging context 624
cca radius user-password 625
charging-action-override 626
charging-rule-optimization 628
check-point accounting 630
constituent-policies 632
content-filtering category policy-id 634
content-filtering flow-any-error 636
content-filtering mode 637
credit-control-group 639
description 641
dynamic-rule order 642
edr edr-dcca-fh 643
edr p2p 645
edr nemo-call 647
edr sn-charge-volume 649
edr suppress-zero-byte-records 651
edr transaction-complete 652
edr voip-call-end 654
egcdr inactivity-meter 656
egcdr cdr-encoding 657
egcdr tariff 659
egcdr threshold 661
egcdr time-duration algorithm 663
end 665
exit 666
extract-host-from-uri 667
firewall dos-protection 669
firewall flooding 672
firewall icmp-destination-unreachable-message-threshold 674
firewall max-ip-packet-size 676
firewall mime-flood 678
firewall no-ruledef-matches 680
firewall policy 683
firewall priority 685
firewall tcp-first-packet-non-syn 689
firewall tcp-idle-timeout-action 690
firewall tcp-reset-message-threshold 691
firewall tcp-syn-flood-intercept 693
flow any-error 695
flow control-handshaking 697
flow end-condition 699
flow limit-across-applications 702
flow rtsp-all-pkts 704
fw-and-nat default-policy 706
http header-parse-limit 708
ip reassembly-timeout 710
ip reset-tos 711
nat binding-record 712
nat policy 714
nat suppress-aaa-update call-termination 716
override-control 717
p2p dynamic-flow-detection 720
pcp service 721
post-processing dynamic 722
post-processing policy 724
post-processing priority 726
qos-renegotiate timeout 728
radius threshold 729
retransmissions-counted 731
ran bandwidth optimize 732
route priority 734
rtp dynamic-flow-detection 739
rtsp initial-bytes-limit 740
ruleddef-parsing 741
tcp 2msl-timeout 743
tcp check-window-size 745
tcp mss 746
tcp out-of-order-timeout 748
tcp packets-out-of-order 749
tcp proxy-mode 752
tethering-detection 754
tft-notify-ue-def-bearer 756
timestamp rounding 757
tpo default-policy 759
transactional-rule-matching 760
transport-layer-checksum 762
udr threshold 764
udr trigger 766
url-blacklisting action 768
url-preprocessing 770
video optimization-preprocessing cae-readdressing 771
websocket flow-detection 772
wtp out-of-order-timeout 773
wtp packets-out-of-order 774
xheader-encryption 776

CHAPTER 19

ACS Ruledef Configuration Mode Commands 779
bearer 3gpp apn 790
bearer 3gpp imsi 792
bearer 3gpp rat-type 794
bearer 3gpp sgsn-address 796
bearer 3gpp2 bsd 798
bearer 3gpp2 service-option 800
bearer apn 802
bearer imsi 804
bearer rat-type 806
bearer sgsn-address 808
bearer traffic-group 810
cca quota-state 812
cca redirect-indicator 814
copy-packet-to-log 816
description 817
dns answer-name 818
dns any-match 820
dns previous-state 822
dns query-name 824
dns return-code 826
dns state 828
dns tid 830
email 832
end 835
exit 836
file-transfer any-match 837
http cookie 908
http domain 910
http error 912
http first-request-packet 914
http header-length 916
http host 918
http payload-length 921
http pdu-length 923
http previous-state 925
http referer 927
http reply code 930
http reply payload 932
http request method 933
http session-length 935
http state 937
http transaction-length 939
http transfer-encoding 941
http uri 943
http url 946
http user-agent 949
http version 951
http x-header 953
icmp any-match 955
icmp code 957
icmp type 959
icmpv6 any-match 961
icmpv6 code 963
icmpv6 type 965
if-protocol 967
imap any-match 969
imap cc 971
imap command 973
imap content class 975
imap content type 977
imap date 979
imap final-reply 981
imap from 983
imap mail-size 985
imap mailbox-size 987
imap message-type 989
imap previous-state 991
imap session-length 993
imap session-previous-state 995
imap session-state 997
imap state 999
imap subject 1001
imap to 1003
ip any-match 1005
ip dscp 1007
ip downlink 1009
ip dst-address 1011
ip error 1013
ip protocol 1015
ip server-domain-name 1017
ip server-ip-address 1019
ip src-address 1021
ip subscriber-ip-address 1023
ip total-length 1025
ip uplink 1027
ip version 1029
mms any-match 1030
mms bcc 1032
mms cc 1034
mms content-location 1036
mms content-type 1038
mms downlink 1040
mms from 1042
mms message-id 1044
mms pdu-type 1046
mms previous-state 1048
sdp connection-ip-address 1196
sdp media-audio-port 1198
sdp media-video-port 1200
sdp uplink 1202
secure-http any-match 1204
secure-http uplink 1206
sip any-match 1208
sip call-id 1210
sip content length 1212
sip content type 1214
sip from 1216
sip previous-state 1218
sip reply code 1220
sip request method 1222
sip request packet 1224
sip state 1226
sip to 1228
sip uri 1230
smtp any-match 1232
smtp command arguments 1234
smtp command id 1236
smtp command name 1238
smtp mail-size 1240
smtp pdu-length 1242
smtp previous-state 1244
smtp recipient 1246
smtp reply arguments 1248
smtp reply id 1250
smtp reply status 1252
smtp sender 1254
smtp session-length 1256
smtp state 1258
tcp analyzed out-of-order 1260
tcp any-match 1262
tcp client-port 1264
tcp connection-initiator 1266
tcp downlink 1267
tcp dst-port 1269
tcp duplicate 1271
tcp either-port 1273
tcp error 1275
tcp flag 1277
tcp initial-handshake-lost 1279
tcp payload 1281
tcp payload-length 1282
tcp previous-state 1284
tcp proxy-prev-state 1286
tcp proxy-state 1288
tcp server-port 1290
tcp session-length 1292
tcp src-port 1294
tcp state 1296
tcp uplink 1298
tethering-detection 1300
tftp any-match 1302
tftp data-any-match 1304
tls 1306
udp any-match 1308
udp client-port 1310
udp downlink 1312
udp dst-port 1314
udp either-port 1316
udp payload starts-with 1318
udp server-port 1319
udp src-port 1321
udp uplink 1323
wsp any-match 1325
wsp content type 1327
wsp domain 1329
wsp downlink 1331
www host 1398
www payload-length 1400
www pdu-length 1402
www previous-state 1404
www reply code 1406
www state 1408
www transfer-encoding 1410
www url 1412

CHAPTER 20
ACS Service Scheme Configuration Mode Commands 1415
  end 1416
  exit 1417
  trigger 1418

CHAPTER 21
ACS Service Scheme Trigger Configuration Mode Commands 1419
  end 1420
  exit 1421
  priority 1422

CHAPTER 22
ACS Subscriber Base Configuration Mode Commands 1425
  end 1426
  exit 1427
  priority 1428

CHAPTER 23
ACS Subscriber Class Configuration Mode Commands 1431
  any-match 1432
  apn 1433
  end 1434
  exit 1435
  multi-line-or 1436
  rulebase 1437
  v-apn 1438

CHAPTER 24
ACS Timedef Configuration Mode Commands 1439
  end 1440
accounting mode 1489
active-charging rulebase 1490
address-resolution-mode 1492
apn-resolve-dns-query 1494
apn-restoration 1495
apn-type 1497
associate accounting-policy 1499
associate qos-mapping 1500
associate quality-of-service-profile 1501
associate sgw-paging-profile 1503
c 1504
dedicated-bearers 1506
description 1508
dhcp lease 1509
direct-tunnel 1511
dns 1512
dns-extn 1514
d 1517
gateway-address 1519
gateway-selection 1521
gn-gtp-version 1523
gtp 1525
idle-mode-acl 1527
ip 1529
ip access-group 1532
ip address pool 1533
ip context-name 1534
isr-sequential-paging 1535
ipv6 1536
local-offload 1538
location-reporting 1539
mobility-protocol 1540
nts 1541
overcharge-protection 1543
pdp-data-inactivity  1545
pdp-type-ipv4v6-override  1547
pgw-address  1548
qos allow-upgrade  1550
qos apn-ambr  1552
qos class  1553
qos dedicated-bearing  1560
qos default-bearing  1561
qos pgw-upgrade  1563
qos prefer-as-cap  1565
qos rate-limit direction  1567
ranap allocation-retention-priority-ie  1572
restrict access-type  1575
sm t3396  1577
timeout bearer-inactivity  1579
timeout idle  1581

twan  1583
virtual-mac  1584

CHAPTER 30  
APN Configuration Mode Commands  1587

aaa  1592
access-link  1594
accounting-mode  1596
active-charging bandwidth-policy  1599
active-charging link-monitor tcp  1601
active-charging radio-congestion  1603
active-charging rulebase  1605
active-charging rulebase-list  1607
apn-ambr  1609
associate accounting-policy  1612
associate qci-qos-mapping  1613
authentication  1615
authorize-with-hss  1620
bearer-control-mode  1622
backoff timer-mode  1624
bearer-duration-stats 1626
cc-home 1627
cc-profile 1629
cc-roaming 1631
cc-sgsn 1633
cc-visiting 1636
content-filtering category 1638
credit-control-client 1640
credit-control-group 1642
daf-pdp-type 1644
data-tunnel mtu 1646
data-tunneling ignore df-bit 1647
dcca origin endpoint 1649
dcca peer-select 1650
description 1652
dhcp context-name 1653
dhcp lease-expiration-policy 1654
dhcp service-name 1655
dhcpv6 context-name 1656
dhcpv6 service-name 1657
dns 1658
egtp 1660
egtpc-qci-stats 1662
ehrpd-access 1664
emergency-apn 1665
end 1666
exit 1667
firewall policy 1668
fw-and-nat policy 1670
gsm-qos negotiate 1672
gtpp group 1674
gtpp secondary-group 1676
idle-timeout-activity 1678
ignore-alt-config 1679
ikev2 tsr 1681
mobile-ip required 1740
mobile-ip reverse-tunnel 1741
nai-construction 1742
nbns 1744
network-behind-mobile 1746
nexthop-forwarding-address 1748
npu qos 1749
outbound 1751
paging-policy-differentiation 1753
p-cscf 1755
pco-options 1757
pdn-behavior 1759
pdp-type 1761
permission 1763
pgw fqdn 1765
policy 1767
ppp 1769
proxy-mip 1771
qci 1773
qos negotiate-limit 1775
qos rate-limit 1778
qos-renegotiate 1781
qos traffic-police 1782
radius 1783
radius group 1784
radius returned-framed-ip-address 1785
radius returned-username 1787
radius rulebase-format 1789
reporting-action 1791
restriction-value 1792
secondary ip pool 1794
selection-mode 1795
stats-profile 1797
timeout 1799
timeout bearer-inactivity 1801
timeout emergency-inactivity 1804
timeout idle 1806
timeout idle micro-checkpoint-deemed-idle 1808
timeout idle micro-checkpoint-periodicity 1810
timeout long-duration 1812
tpo policy 1814
tunnel address-policy 1815
tunnel gre 1817
tunnel ipip 1819
tunnel ipsec 1821
tunnel l2tp 1822
virtual-apn gdcr 1825
virtual-apn preference 1827

CHAPTER 31 APN Remap Table Configuration Mode 1835
apn-remap 1837
apn-selection-default 1840
blank-apn 1844
cc 1845
description 1847
end 1848
exit 1849
wildcard-apn 1850

CHAPTER 32 ARP-RP Mapping Profile Configuration Mode 1853
arp 1854
end 1856
exit 1857

CHAPTER 33 ATM Port Configuration Mode Commands 1859
clock-source 1861
description 1862
end 1863
exit 1864
line-timing 1865
loopback 1866
preferred slot 1868
pvc 1870
shutdown 1872
snmp trap link-status 1873
threshold high-activity 1874
threshold monitoring 1876
threshold rx-utilization 1878
threshold tx-utilization 1880
toh-sdsf 1882

CHAPTER 34
Bearer Control Profile Configuration Mode Commands 1885
dedicated-bearer 1886
default-bearer 1890
description 1894
end 1895
exit 1896
pre-rel8-qos-mapping 1897

CHAPTER 35
BFD Configuration Mode Commands 1899
bfd linkagg-peer 1900
bfd multihop-peer 1902
bfd nbr-group-name 1904
echo 1906
end 1907
exit 1908
slow-timers 1909

CHAPTER 36
BGP Address-Family (IPv4/IPv6) Configuration Mode Commands 1911
dedicated-bearer 1886
default-bearer 1890
description 1894
end 1895
exit 1896
maximum-paths 1914
neighbor 1916
network 1920
redistribute 1921
timers bgp 1923

CHAPTER 37

BGP Address-Family (VPNv4/VPNv6) Configuration Mode Commands 1925

end 1926
exit 1927
neighbor 1928
timers bgp 1930

CHAPTER 38

BGP Address-Family (VRF) Configuration Mode Commands 1931

end 1932
exit 1933
neighbor 1934
redistribute 1938

CHAPTER 39

BGP Configuration Mode Commands 1941

accept-zero-as-rd 1943
address-family ipv4 1944
address-family ipv6 1946
address-family vpn4 1947
address-family vpn6 1948
bgp 1949
description 1950
distance 1951
end 1953
enforce-first-as 1954
exit 1955
ip vrf 1956
maximum-paths 1957
neighbor 1958
network 1963
redistribute 1964
router-id 1966
scan-time 1967
timers 1968
CHAPTER 40  BGP IP VRF Configuration Mode Commands  1971
  end  1972
  exit  1973
  route-distinguisher  1974
  route-target  1976

CHAPTER 41  BITS Port Configuration Mode Commands  1979
  default  1980
  description  1981
  end  1982
  exit  1983
  mode  1984
  preferred slot  1985
  recover  1986
  shutdown  1988
  snmp trap link-status  1989

CHAPTER 42  BMSC Profile Configuration Mode Commands  1991
  end  1992
  exit  1993
  gmb diameter dictionary  1994
  gmb diameter endpoint  1995
  gmb diameter peer-select  1996
  gmb user-data  1998

CHAPTER 43  BSSGP Cause Code Group Configuration Mode  2001
  end  2002
  exit  2003
  radio-cause  2004

CHAPTER 44  Bulk Statistics File Configuration Mode Commands  2007

CHAPTER 45  Bulk Statistics Configuration Mode Commands  2009
  Overview  2013
Contents

Schema Format String Syntax 2013
Schema Format String Length 2013
Bulk Statistic Variables 2013
aal2 schema 2014
alcap schema 2016
apn schema 2018
asngw schema 2020
bmcms schema 2022
card schema 2024
closedrp schema 2026
context schema 2028
cs-network-ranap schema 2030
cs-network-rtp schema 2032
cs-network-sccp schema 2034
deca schema 2036
deca-group schema 2038
default 2040
diameter-acct schema 2042
diameter-auth schema 2044
dlci-util schema 2046
dpca schema 2048
ecs schema 2050
egtpc schema 2052
dr 2054
exit 2055
fa schema 2056
file 2058
fng schema 2060
footer 2061
gather-on-standby 2063
gprs schema 2064
gtpc schema 2066
gtpp schema 2068
gtpu schema 2070
ha schema 2072
header 2074
hnbgw-hnbp schema 2076
hnbgw-hnbp-access-closed schema 2078
hnbgw-hnbp-access-hybrid schema 2080
hnbgw-hnbp-access-open schema 2082
hnbgw-ranap schema 2084
hnbgw-ranap-access-closed schema 2086
hnbgw-ranap-access-hybrid schema 2088
hnbgw-ranap-access-open schema 2090
hnbgw-rtp schema 2092
hnbgw-rtp-access-closed schema 2094
hnbgw-rtp-access-hybrid schema 2096
hnbgw-rtp-access-open schema 2098
hnbgw-rua schema 2100
hnbgw-rua-access-closed schema 2102
hnbgw-rua-access-hybrid schema 2104
hnbgw-rua-access-open schema 2106
hnbgw-sctp schema 2108
hsgw schema 2110
hss schema 2112
icsr schema 2114
imsa schema 2116
ippool schema 2118
ipsg schema 2120
lac schema 2122
limit 2124
link-aggr schema 2125
lma schema 2127
lns schema 2129
mag schema 2131
mipv6ha schema 2133
mme schema 2135
mvs schema 2137
nat-realm schema 2139
p2p schema 2141
Contents

- vlan-npu schema 2213
- vrf schema 2215
- wsg schema 2217
About this Guide

This preface describes the Command Line Interface Reference and its document conventions.
This reference describes how to use the command line interface (CLI) to interact with the products supported by the StarOS™. The CLI commands are organized by command modes in the code and in this reference. The command modes are presented alphabetically. The description of each command states the command's function, describes its syntax, presents limitations when applicable, and offers an example of its usage.

- CLI Command Sections, page xli
- Supported Documents and Resources, page xlii

CLI Command Sections

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

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

**Supported Documents and Resources**
Related Common Documentation

The following common documents are available:

• AAA Interface Administration Reference
• GTPP Interface Administration Reference
• Installation Guide (platform dependant)
• Release Change Reference
• SNMP MIB Reference
• Statistics and Counters Reference
• System Administration Guide (platform dependant)
• Thresholding Configuration Guide
Related Product Documentation

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

The following related product documents are also available:

- ADC Administration Guide
- CF Administration Guide
- ECS Administration Guide
- ePDG Administration Guide
- eWAG Administration Guide
- GGSN Administration Guide
- HA Administration Guide
- HeNB-GW Administration Guide
- HNB-GW Administration Guide
- HSGW Administration Guide
- InTracer Installation and Administration Guide
- IPSec Reference
- IPSG Administration Guide
- MME Administration Guide
- MURAL Installation and Administration Guide
- MURAL User Guide
- MVG Administration Guide
- NAT Administration Guide
- P-GW Administration Guide
- PDSN Administration Guide
- PSF Administration Guide
- S-GW Administration Guide
- SAEGW Administration Guide
- SaMOG Administration Guide
- SCM Administration Guide
- SecGW Administration Guide
- SGSN Administration Guide
Obtaining Documentation

The most current Cisco documentation is available on the following website:
http://www.cisco.com/cisco/web/psa/default.html

Use the following path selections to access this documentation:
Products > Wireless > Mobile Internet> Platforms > Cisco ASR 5000 Series > Cisco ASR 5000
Command Line Interface Overview

This chapter describes the numerous features in the command line interface (CLI). It includes 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 (StarOS™) 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, page 2
- CLI Command Modes, page 2
- CLI Administrative Users, page 2
- CLI Contexts, page 9
- Understanding the CLI Command Prompt, page 10
- CLI Command Syntax, page 11
- Entering and Viewing CLI Commands, page 11
- Obtaining CLI Help, page 16
- Exiting the CLI and CLI Command Modes, page 16
- Accessing the CLI, page 17
- Platform Related CLI Issues, page 18
- Trusted Builds, page 19
- IP Address Notation, page 19
- Alphanumeric Strings, page 21
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.

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 to the user vary based on platform type, StarOS 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 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 or TACACS+ server. Passwords for these user types are assigned once and are accessible in the configuration file.
• **Local-users**: This user type supports ANSI T1.276-2003 password security protection. Local-user account information, such as passwords, password history, and lockout states, is maintained in /flash. This information is maintained in a separate local user database subject to AAA based authentication and is not used by the rest of the system. As such, configured local-user accounts are not visible with the rest of the system configuration.

---

**Important**

In release 20.0 and higher Trusted StarOS builds, the local user database is disabled. The Global Configuration mode `local-user` commands, and Exec mode `show local-user` and `update local-user` commands are unavailable. For additional information on Trusted builds, see the System Administration Guide.

Local-user and context-level administrative accounts can be used in parallel. However, a mechanism is provided to de-activate 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) SN-Admin-Permission or SN1-Admin-Permission.

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

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

- None = 0
- CLI = 1
- FTP = 2
- CLI-FTP = 3
- Intercept = 4
- CLI-Intercept = 5
- CLI-Interceptor-FTP = 7
- ECS = 8
- CLI-ECS = 9
- CLI-FTP-ECS = 11
- CLI-Interceptor-ECS = 13
- CLI-Interceptor-FTP-ECS = 15

The default value is 1 (CLI).
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 supported attribute/value mapping system that is constant, regardless of server manufacturer or model:

Table 1: RADIUS Attribute/Value Mapping System

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Framed</td>
<td>2</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>Authorize Only</td>
<td>17</td>
</tr>
<tr>
<td>Inspector</td>
<td>19650516</td>
</tr>
<tr>
<td>Security_Admin</td>
<td>19660618</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>

Authenticating Administrative Users with TACACS+

The ASR 5x00 or StarOS virtual machine is identified as a Network Access Server (NAS) and remotely accesses the Terminal Access Controller Access Control System+ (TACACS+) server for information about users who can perform administrative operations on the system.

The NAS is defined as a client-side requesting component associated with a specific IP address. StarOS only supports one NAS with one IP address. This NAS processes TACACS+ protocol packets within the local context. Several management services may be associated with a login.
StarOS only supports multiple-connection mode with a TACACS+ server. In a multiple-connection mode, each TACACS+ session opens and maintains a separate and private TCP connection to the server. When the session ends, this connection is always closed.

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

**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*

![User Privileges Diagram]

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.

---

**Important**

In release 20.0 and higher Trusted StarOS builds, the Global Configuration mode `local-user` commands are unavailable.

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. This section defines the commands allowed for each management user type.
**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
- 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)
Allowed Commands per User Type

- debug
- dhcp test
- gtpc test
- gtpp interim
- gtp test
- gtpu test
- gtpv0 test
- host
- logging active
- logging filter
- logging trace
- monitor protocol
- monitor subscriber
- 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 Configuration Mode:
  - config-administrator
  - operator
  - inspector
  - administrator

- Global Configuration 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*
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**: 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.

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

```plaintext
show port info slot_number/port_number
```

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

A keyword that was supported in a previous release may be concealed in subsequent releases. StarOS continues to parse concealed keywords in existing scripts and configuration files created in a previous release. But the concealed keyword no longer appears in the command syntax for use in new scripts or configuration files. Entering a question mark (?) will not display a concealed keyword as part of the Help text.

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.

If you enter the partial command `conf` and press Enter, you enter the Global Configuration Mode. If you were to enter only `c`, 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.

```
[local] host_names show<Tab>
[local] host_names 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:

```
[local] host_names sh<Tab>

[local] host_names#
```

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

```
[local] host_names sh
shutdown - Terminates execution of all tasks within the entire chassis
show - Displays information based on a specified argument
[local] host_names#
```

### Important

If you enter a partial keyword for a keyword that is concealed in this release, pressing Tab will not complete the concealed keyword. You must type in the complete keyword to display/execute a concealed keyword.

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

Entering "?" will not display keywords that have been concealed in this release.

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: |

```
[local] host_names 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.
For example, to save 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.

You create a context named `newcontext`:

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

You revisit the context named `newcontext`:

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

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

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

After aborting the above action, you can again revisit `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 Configuration 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.
grep for Regular Expressions

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

### Table 4: grep Options

<table>
<thead>
<tr>
<th>Alternative Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-E</td>
<td>Match using extended regular expressions (EREs). Treat each pattern specified as an ERE (&quot;IEEE Std 1003.1-2001, Section 9.4, Extended Regular Expressions&quot;). If any entire ERE pattern matches some part of an input line excluding the terminating &lt;newline&gt;, the line shall be matched. A null ERE shall match every line.</td>
</tr>
<tr>
<td>-i</td>
<td>Perform pattern matching in searches without regard to case. Lower case matches the same as upper case.</td>
</tr>
<tr>
<td>-n</td>
<td>Precede each output line by its relative line number in the file, each file starting at line 1. The line number counter is reset for each file processed.</td>
</tr>
<tr>
<td>-v</td>
<td>Select lines not matching any of the specified patterns. If the -v option is not specified, selected lines shall be those that match any of the specified patterns.</td>
</tr>
<tr>
<td>--extended-regexp</td>
<td>The long form of the -E option.</td>
</tr>
<tr>
<td>--ignore-case</td>
<td>The long form of the -i option.</td>
</tr>
<tr>
<td>--invert-match</td>
<td>The long form of the -v option.</td>
</tr>
<tr>
<td>expression</td>
<td>Specifies the character pattern to find in the command's output as an alphanumeric string of 1 to 256 characters.</td>
</tr>
</tbody>
</table>

A regular expression is a pattern that describes a set of strings. Regular expressions are constructed analogously to arithmetic expressions, by using various operators to combine smaller expressions. For additional information, refer to ISO/IEC/IEEE 9945:2009 Information technology – Portable Operating System Interface (POSIX®) Base Specifications, Issue 7.
more Command

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><code>&lt;Ctrl + p&gt;</code> and <code>&lt;up arrow&gt;</code></td>
<td>Recalls previous command in the command history</td>
</tr>
<tr>
<td><code>&lt;Ctrl + n&gt;</code> and <code>&lt;down arrow&gt;</code></td>
<td>Recalls next command in the command history</td>
</tr>
<tr>
<td><code>&lt;Ctrl + f&gt;</code> and <code>&lt;right arrow&gt;</code></td>
<td>Moves cursor forward by one character in command line</td>
</tr>
<tr>
<td><code>&lt;Ctrl + b&gt;</code> and <code>&lt;left arrow&gt;</code></td>
<td>Moves cursor backward by one character in command line</td>
</tr>
<tr>
<td><code>&lt;Esc&gt; + &lt;f&gt;</code></td>
<td>Moves cursor forward by one word in command line</td>
</tr>
<tr>
<td><code>&lt;Esc&gt; + &lt;b&gt;</code></td>
<td>Moves cursor backward by one word in command line</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;a&gt;</code></td>
<td>Moves cursor to the beginning of the command line</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;e&gt;</code></td>
<td>Moves cursor to the end of the command line</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;k&gt;</code></td>
<td>Deletes the current command line from the insertion point to the end of the line</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;u&gt;</code></td>
<td>Deletes the current command line from the insertion point to the beginning of the line</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;d&gt;</code></td>
<td>Deletes a single character in the current command line</td>
</tr>
<tr>
<td><code>&lt;Esc&gt; + &lt;d&gt;</code></td>
<td>Deletes a word in the current command line</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;c&gt;</code></td>
<td>Quits editing the current line</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;l&gt;</code></td>
<td>Refreshes the display</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;t&gt;</code></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 access help.
  
  `[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 (?).
  
  `[local]host_name# test alarm?`
  
  `audible - Tests internal audible alarm buzzer on SPC`
  `central-office - Tests specified central office alarm relays`
  `<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 (?).
  
  `[local]host_name# show card info?`
  
  `<Enter card number as an integer ranging 1 to n>`
  `| - 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.

```
[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.

```
[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 Exec Mode prompt.

**Accessing the CLI**

Access the CLI through the following methods:

- Local login through an ASR 5x00 Console port via a serial connection with a management card
- Local login through a vConsole port via the hypervisor that initiated the StarOS virtual machine
- Remote login using Telnet and Secure Shell (SSH) access to the CLI through any IP interface on the system. You can use remote login methods only after the system has been configured to support the various access methods.

**Important**

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

Multiple CLI sessions are supported, but the number of sessions varies based on the amount of available memory. The Resource Manager reserves enough resources so that as a minimum up to 15 CLI sessions are assured. One of the CLI sessions is always reserved for use exclusively by a CLI session on a Console or vConsole interface. Additional CLI sessions beyond the pre-reserved set are permitted if sufficient CPU or vCPU 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 an ASR 5x00 Console Port**

This section provides instructions for accessing the CLI locally through a Console port on the ASR 5x00 platform.

Establish a connection between the serial Console port on an ASR 5x00 and a workstation that has a communications application that accesses the workstation's serial port, such as Minicom for Linux or HyperTerminal® for MicroSoft Windows®. Refer to the ASR 5x00 Installation Guide for detailed information on connecting to a serial Console port.

1. Configure the communications application to support the following:
### Accessing the CLI Locally Using a vConsole Port

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

### 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 in the System Administration Guide.

### Platform Related CLI Issues

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

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

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

---

<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.

2. At the terminal window, press Enter.
3. 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.
Trusted Builds

A Trusted build is a starfile image from which non-secure or low security features have been deleted or disabled. However, the binaries in the Trusted starfile image are are identical to those found in other starfiles for a particular StarOS release-build number. In general, a Trusted build is more restrictive than a Normal build image.

You can identify whether your platform is running a Trusted build via the Exec mode `show version` command. The output of the command displays the word "Trusted" as part of the image description text.

The following non-secure programs and features are disabled/removed from a Trusted build:

- Telnet
- FTP (File Transfer Protocol)
- Local user database access
- `tcpdump` utility
- `rlogin` (Remote Login) utility and `rlogind` (Remote Login daemon)
- `rsh` (Remote Shell) and `rcp` (Remote Copy) utilities

IP Address Notation

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

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

IPv4 Dotted-Decimal Notation

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

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

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

IPv6 Colon-Separated-Hexadecimal Notation

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

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

The hexadecimal digits are case-insensitive.
The 128-bit IPv6 address can be abbreviated with the following rules:

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

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

### CIDR Notation

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

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

CIDR notation is constructed from the IP address and the prefix size, the latter being the number of leading 1 bits of the routing prefix. The IP address is expressed according to the standards of IPv4 or IPv6. It is followed by a separator character, the slash (/) character, and the prefix size expressed as a decimal number.

---

**Important**

On the ASR 5000, routes with IPv6 prefix lengths less than /12 and between the range of /64 and /128 are not supported.

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

For example:

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

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

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

Character Set

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

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

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

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

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

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

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

interface "Rack 3 Chassis 1 port 5/2"
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.

Command Modes

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

config > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

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

Important

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

- description, page 25
- diameter accounting, page 26
- diameter authentication, page 30
- diameter authentication failure-handling, page 34
- diameter authentication failure-handling-template, page 36
- diameter authentication strip-leading-digit, page 38
- diameter dictionary, page 40
- end, page 41
- exit, page 42
- radius, page 43
- radius accounting, page 48
• radius accounting apn-to-be-included, page 52
• radius accounting algorithm, page 53
• radius accounting billing-version, page 55
• radius accounting gtp trigger-policy, page 56
• radius accounting ha policy, page 58
• radius accounting interim, page 60
• radius accounting ip remote-address, page 62
• radius accounting keepalive, page 64
• radius accounting pdif trigger-policy, page 67
• radius accounting rp, page 68
• radius accounting server, page 71
• radius algorithm, page 75
• radius allow, page 76
• radius attribute, page 78
• radius authenticate, page 84
• radius authenticator-validation, page 86
• radius charging, page 87
• radius charging accounting algorithm, page 90
• radius charging accounting server, page 92
• radius charging algorithm, page 95
• radius charging server, page 96
• radius ip vrf, page 99
• radius keepalive, page 101
• radius mediation-device, page 104
• radius probe-interval, page 105
• radius probe-max retries, page 106
• radius probe-timeout, page 107
• radius server, page 108
• radius trigger, page 112
description

Allows you to enter descriptive text for this configuration.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

description text

no description

**no**

Clears the description for this configuration.

text

Enter descriptive text as an alphanumeric string of 1 to 100 characters.

If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

**Usage Guidelines**

The description should provide useful information about this configuration.
diameter accounting

This command configures Diameter accounting parameters.

Product
All

Privilege
Security Administrator, Administrator

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

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-aaa-group)>

Syntax Description
diameter accounting {dictionary {aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq | rf-plus } | endpoint endpoint_name | hd-mode fall-back-to-local | hd-storage-policy hd_policy | max-retries max_retries | max-transmissions max_transmissions | request-timeout request_timeout_duration | sdc-integrity | server host_name priority priority | upgrade-dict-avps {3gpp-rel10 | 3gpp-rel9} }
default diameter accounting {dictionary | hd-mode | max-retries | max-transmissions | request-timeout | upgrade-dict-avps }
no diameter accounting {endpoint | hd-mode | hd-storage-policy | max-retries | max-transmissions | sdc-integrity | server host_name | upgrade-dict-avps }

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

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 hard disk drive (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.

sdc-integrity: Excludes the "SDC-Integrity-Grouping" Diameter AVP in the ACR message even if present in the "aaa-custom4" dictionary.

server host_name: Removes the configured Diameter host host_name from this AAA server group for Diameter accounting.
**upgrade-dict-avps**: Sets the release version to 3GPP Rel. 8 for upgrading Diameter accounting dictionary in the current AAA group.

**default diameter accounting**: Setsthecontext'sdictionaryasthesystemdefault.

**dictionary**: 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.

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

**dictionary**: Specifies the Diameter accounting dictionary.

**aaa-custom1 ... aaa-custom10**: Configures 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.

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

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

**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.

**hd-mode**

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**

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 an alphanumeric string of 1 through 63 characters.

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 max_retries**

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

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

Default: 0

**max-transmissions max_transmissions**

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

*max_transmissions* must be an integer from 1 through 1000.

Default: 0

**request-timeout request_timeout_duration**

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

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

Default: 20

**sdc-integrity**

This keyword enables the SDC Integrity feature. When enabled, SDC-Integrity-Grouping AVP is included in the ACR message. This AVP contains the number of Service Data Containers (SDCs) included by P-GW and the checksum as calculated by the previously defined algorithm. The checksum calculation is done only if the AVP is included. By default, this feature is disabled i.e. the grouped AVP is not included in the ACR message even if present in the "aaa-custom4" dictionary. The CLI command will have no effect if the dictionary does not contain the SDC-Integrity-Grouping AVP.

---

**Important**

This feature is customer-specific. For more information, contact your Cisco Account representative.

---

P-GW generates the charging data and creates a new ACR with individual SDCs based on Rating Groups, and then sends the ACR message directly to Charging Collection Function (CCF). When an intermediate node is inserted between P-GW and CCF, the node appends more SDCs in the charging record sent by P-GW through the Rf interface.

To protect the integrity of SDCs, P-GW counts the number of SDCs, runs a checksum algorithm against the bytes within the SDCs, and then adds the "SDC-Integrity-Grouping" AVP with these two values in the ACR message. This grouped AVP is optional and defined in "aaa-custom4" dictionary only. This vendor-specific AVP can be enabled only when the peer supports the vendor ID. This feature helps CCF to distinguish the SDCs included by the intermediate node.

For this feature to work, the CLI control must be enabled and "aaa-custom4" dictionary containing the grouped AVP should be used and associated with the appropriate AAA group. When this feature is enabled, there might be minimal performance impact on P-GW specifically on AAA Manager tasks due to checksum calculation.
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 an alphanumeric string of 1 through 63 characters.
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.

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

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

Examples
The following command configures the Diameter accounting dictionary, aaa-custom10:
diameter accounting dictionary aaa-custom10
The following command configures the Diameter endpoint, EAP1:
diameter accounting endpoint EAP1
The following commands configure Diameter accounting options:
diameter accounting max-retries 4
diameter accounting max-transmissions 2
diameter accounting request-timeout 10
diameter accounting server svc priority 1
diameter authentication

This command configures Diameter authentication parameters.

Product All

Privilege Security Administrator, Administrator

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

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

<context_name>host_name(config-aaa-group)#

Syntax Description

- **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 | dynamic-load | nasreq } | encode-supported-features | endpoint endpoint_name | max-retries max_retries | max-transmissions max_transmissions | redirect-host-avp { just-primary | primary-then-secondary } | request-timeout request_timeout_duration | server host_name priority priority | upgrade-dict-avps { 3gpp-rel10 | 3gpp-rel9 } |
- **no diameter authentication { dictionary | encode-supported-features | max-retries | max-transmissions | redirect-host-avp | request-timeout | upgrade-dict-avps }
- **no diameter authentication { encode-supported-features | endpoint | max-retries | max-transmissions | server host_name | upgrade-dict-avps }
- **encode-supported-features**: Disables the CLI command to not send the Supported-Features AVP.
- **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.
- **upgrade-dict-avps**: Sets the release version to 3GPP Rel. 8 for upgrading Diameter authentication dictionary in the current AAA group.
default diameter authentication { dictionary | encode-supported-features | max-retries | max-transmissions | redirect-host-avp | request-timeout | upgrade-dict-avps }

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

encode-supported-features: Configures the default setting, that is not to send the Supported-Features AVP in AAR message.

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.

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


Specifies the Diameter authentication dictionary.

aaa-custom1 ... aaa-custom8, aaa-custom10 ... aaa-custom20: Configures 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.

aaa-custom9: Configures the STA standard dictionary.

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

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

encode-supported-features

Encodes Supported-Features AVP.

endpoint endpoint_name

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

endpoint_name must be an alphanumeric string of 1 through 63 characters.
max-retries \textit{max\_retries}

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

\textit{max\_retries} specifies the maximum number of retry attempts, and must be an integer from 1 through 1000.

Default: 0

max-transmissions \textit{max\_transmissions}

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

\textit{max\_transmissions} specifies the maximum number of transmission attempts, and must be an integer from 1 through 1000.

Default: 0

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.

\textit{just-primary}: Redirect only to primary host.

\textit{primary-then-secondary}: Redirect to primary host, if fails then redirect to the secondary host.

Default: just-primary

request-timeout \textit{request\_timeout\_duration}

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

\textit{request\_timeout\_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 \textit{host\_name} priority \textit{priority}

Specifies the current context Diameter authentication server's host name and priority.

\textit{host\_name} specifies the Diameter authentication server's host name, and must be an alphanumeric string of 1 through 63 characters.

\textit{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.

upgrade-dict-avps \{ 3gpp-rel10 | 3gpp-rel9 \}

Specifies to upgrade Diameter authentication dictionary to 3GPP Rel. 9 version or 3GPP Rel. 10 version.

\textit{3gpp-rel10}: Upgrades the dictionary to 3GPP Rel. 10 version.

\textit{3gpp-rel9}: Upgrades the dictionary to 3GPP Rel. 9 version.

Default: Sets the release version to 3GPP Rel. 8
Usage Guidelines

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

Examples

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

```
diameter authentication dictionary aaa-custom1
```

The following command configures the Diameter endpoint, `EAP1`:

```
diameter authentication endpoint EAP1
```

The following commands configure Diameter authentication options:

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

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

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

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

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-aaa-group)#
```

**Syntax Description**

```
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 } } }
no 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 the session
- **retry-and-terminate**: First retries, if it fails then terminates the session
- **terminate**: Terminates the session

---

**Important**

For any failure encountered, the "continue" option terminates the call as with the "terminate" option for all Diameter dictionaries except aaa-custom15 dictionary.

---

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 the action to be taken for failures:

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

---

**Important**

For any failure encountered, the "continue" option terminates the call as with the "terminate" option for all Diameter dictionaries except aaa-custom15 dictionary. This behavior is true in releases prior to 20. In 20 and later releases, the "continue" option is applicable for all S6b dictionaries including aaa-custom15 dictionary.

---

**Usage Guidelines**

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.

**Examples**

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 authentication failure-handling-template

This command associates the failure-handling template with AAA group authentication for Diameter authentication requests and Diameter Extensible Authentication Protocol (EAP) requests.

Product

- ePDG
- P-GW

Privilege

Security Administrator, Administrator

Command Modes

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

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-aaa-group)#

Syntax Description

diameter authentication failure-handling-template template_name

no diameter authentication failure-handling-template

no

Disassociates a failure handling template with the AAA group authentication.

failure-handling-template template_name

Associates a previously created failure handling template with the authentication application in the AAA group. template_name specifies the name for a pre-configured failure handling template. template_name must be an alphanumeric string of 1 through 63 characters. By default, the template is not associated in the AAA group.

For more information on failure handling template, refer to the failure-handling-template command in the Global Configuration Mode Commands chapter.

Usage Guidelines

Use this command to associate a configured failure handling template with the AAA group authentication application. The failure handling template defines the action to be taken when the Diameter application encounters a failure supposing a result-code failure, Tx-expiry or response-timeout. The application will take the action given by the template. For more information on failure handling template configurations, refer to the Diameter Failure Handling Template Configuration Mode Commands chapter in this guide.

This CLI command is introduced to support Overload Control on Diameter interfaces such as Gx, S6b and SWm and also to prevent network overload and outages. Whenever there is an overload condition at the
Diameter Servers or DRA and request times out, the clients (ePDG/P-GW) are typically unaware of the overload condition and attempt to send the message on an alternate connection with the Diameter server causing some more traffic in the network. In order to handle this overload condition effectively, a new vendor-specific Diameter Experimental Result-Code 5198 (DIAMETER_OVERLOAD_RETRY_NOT_ALLOWED_TO_ANY) is defined.

When the overloaded PCRF/DRA receives a message, it includes the result-code 5198 in the response message. On receiving the experimental result-code, call is terminated based on the failure-handling configuration. If failure-handling is configured as local-policy, then the call is continued with local-policy without retrying the secondary server. For more information on the Diameter Overload Control feature, refer to the AAA Interface Administration and Reference document.

When the failure-handling-template is configured and the failure-handling CLI is also enabled in the AAA Group configuration, the template is given the higher preference. When the Result-Code (5198) is received in DEA/AAA request, the call is terminated without the Session Terminate Request (STR) for S6b and SWm interfaces.

If the association is not made to the template then failure handling behavior configured in the application with the failure-handling command will take its effect.

**Examples**

The following command associates the failure handling template FH_1 with the Diameter authentication interface.

`diameter authentication failure-handling-template FH_1`
**diameter authentication strip-leading-digit**

This command enables or disables stripping of leading digit from User-Name AVP of non-authentication procedures like AAR and STR.

**Product**
- ePDG
- HSGW
- P-GW

**Privilege**
- Security Administrator, Administrator

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

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-aaa-group)#
```

**Syntax Description**

```
[ no ] diameter authentication strip-leading-digit { user-name }
```

- **no**
  - Disables the stripping of leading digit from User-Name AVP of non-authentication procedures

- **user-name**
  - This keyword specifies to strip off the leading digit from User-Name AVP of non-authentication procedures. By default, this feature is disabled.

**Usage Guidelines**

As part of 2015 4G network upgrade release, no leading digit is included in the User-Name AVP of non-authentication procedures like AAR and STR. For backward compatibility, the 3GPP AAA server accepts User-Name with and without the leading digit.

This CLI command is used to control the stripping of leading digit in the User-Name AVP. This feature is applicable to all authentication and authorization interfaces like S6b, STa and SWm and not for accounting interfaces. This CLI command is applicable only for AAR and STR messages.

If the User-Name AVP is received in RAR (for SWm and STa), the same User-Name is included in the RAA message irrespective of the CLI option. For example, if the User-Name AVP is prefixed with 0 in RAR and the CLI option for stripping is enabled, then the User-Name AVP is sent in RAA with the leading "0".
Important

This CLI command will not take effect for aaa-custom17 and aaa-custom19 dictionaries. This CLI is not applicable for response messages (RAA/ASA) sent by chassis.

Examples

The following command strips off the leading digit in the User-Name AVP of non-authentication procedures.

diameter authentication strip-leading-digit user-name
This command is deprecated and is replaced by the diameter accounting dictionary and diameter authentication dictionary commands. See the diameter accounting, on page 26 and diameter authentication, on page 30 commands respectively.
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

**Usage Guidelines**
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 Description**

exit

**Usage Guidelines**

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

This command configures basic RADIUS options.

**Product**  
All

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

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

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
radius { deadtime minutes | detect-dead-server { consecutive-failures consecutive_failures_count | response-timeout response_timeout_duration } | dictionary dictionary | max-outstanding max_messages | max-retries max_retries | max-transmissions max_transmissions | probe-message local-service-address ipv4/ipv6_address | strip-domain { authentication-only | accounting-only } | timeout idle_seconds }
default radius { deadtime | detect-dead-server | dictionary | max-outstanding | max-retries | max-transmissions | timeout }
no radius { detect-dead-server | max-transmissions | radius probe-message local-service-address | strip-domain }
```

**no**

Removes the specified configuration.

**default**

Configures default setting for the specified keyword.

**dictionary dictionary**

Specifies which dictionary to use. The following table describes the 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>Dictionary</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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. Important: In 12.0 and later releases, no new attributes can be added to the starent-vsa1 dictionary. If there are any new attributes to be added, these can only be added to the starent dictionary. For more information, please contact your Cisco account representative.</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>
<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**

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.

Default: 10
This parameter is not applicable when `radius detect-dead-server keepalive` is configured. For keepalive approach `radius keepalive consecutive-response` is used instead of `radius deadtime` to determine when the server is marked as reachable. For further explanation refer to `radius keepalive consecutive-response` command's description.

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.

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

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

`consecutive-failures consecutive_failures_count`: Specifies the number of consecutive failures, for any AAA Manager, before a server's state is changed from "Active" to "Down". `consecutive_failures_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 response_timeout_duration`: 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". `response_timeout_duration` must be an integer from 1 through 65535.

If both `consecutive-failures` and `response-timeout` are configured, then both parameters must be met before a server's state is changed to "Down".

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 max_messages**

Specifies the maximum number of outstanding messages a single AAA Manager instance will queue. `max_messages` must be an integer from 1 through 4000. Default: 256
max-retries \textbf{max\_retries}\linebreak 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.\linebreak \textit{max\_retries} must be an integer from 0 through 65535.\linebreak Default: 5

\textbf{max-transmissions max\_transmissions}\linebreak Sets the maximum number of re-transmissions for RADIUS authentication requests. This limit is used in conjunction with \textbf{max-retries} parameter for each server.\linebreak 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.\linebreak 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.\linebreak \textit{max\_transmissions} must be an integer from 1 through 65535.\linebreak Default: Disabled

\textbf{probe-message local-service-address ipv4/ipv6\_address}\linebreak \textbf{radius probe-message}: Configures AVPs to be sent in RADIUS authentication probe messages.\linebreak \textbf{local-service-address}: Configures the service ip-address to be sent as an AVP in RADIUS authentication probe messages.\linebreak \textit{ipv4/ipv6\_address}: Specifies the IP address of the server.\linebreak \textit{ip\_address} must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

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

\textbf{timeout idle\_seconds}\linebreak Specifies the number of seconds to wait for a response from the RADIUS server before re-sending the messages.\linebreak \textit{idle\_seconds} must be an integer from 1 through 65535.\linebreak Default: 3

\textbf{Usage Guidelines}\linebreak Use this command to configure the basic RADIUS parameters according to the RADIUS server used for the context.
Examples

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

radius timeout 300
radius accounting

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

Product
All

Privilege
Security Administrator, Administrator

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

Entering the above command sequence results in the following prompt:
{context_name}host_name(config-aaa-group)#

Syntax Description
radius accounting { archive | stop-only | | realtime minutes | detect-dead-server { consecutive-failures consecutive_failures_count | keepalive | response-timeout response_timeout_duration | | fire-and-forget | interim interval interim_interval | max-outstanding max_messages | max-pdu-size octets | max-retries max_retries | max-transmissions max_transmissions | timeout idle_seconds }
default radius accounting { archive | detect-dead-server | fire-and-forget | max-outstanding | max-pdu-size | max-retries | max-transmissions | timeout }
no radius accounting { archive | detect-dead-server | fire-and-forget | interim interval | max-transmissions }

no
Removes the specified configuration.

default
Configures the default setting for the specified keyword.

archive | stop-only |
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 serially delivered to the RADIUS accounting server. 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.
Default: enabled
**deadtime 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.

Default: 10 minutes

---

**Important**

This parameter is not applicable when `radius accounting detect-dead-server keepalive` is configured. For keepalive approach `radius accounting keepalive consecutive-response` is used instead of `radius accounting deadtime` to determine when the server is marked as reachable. For further explanation refer to `radius accounting keepalive consecutive-response` command's description.

---

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

---

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

- **consecutive-failures consecutive_failures_count**: Specifies the number of consecutive failures, for any AAA Manager, before a server's state is changed from "Active" to "Down". `consecutive_failures_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: disabled

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

**fire-and-forget**

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

Default: Disabled

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

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

Keepalive feature for server state detection is supported in conjunction since there is no waiting for responses. Archiving in such a AAA group is not supported. If the server is down, the request is sent to the next server in the group. If all the servers in the group are down, the request is deleted.

This CLI is independent of the APN or subscriber profile configuration `aaa secondary-group aaa_group_name`.

**interim interval** *interim_interval*

Specifies the time interval, in seconds, for sending accounting INTERIM-UPDATE records.

`interim_interval` must be an integer from 50 through 40000000.

Default: Disabled

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** *max_messages*

Specifies the maximum number of outstanding messages a single AAA Manager instance will queue.

`max_messages` must be an integer from 1 through 4000.

Default: 256

**max-pdu-size** *octets*

Specifies the maximum sized packet data unit which can be accepted/generated, in bytes (octets).

`octets` must be an integer from 512 through 2048.

Default: 2048
**max-retries max_retries**

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.

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

Default: 5

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 max_transmissions**

Sets the maximum number of transmissions for a RADIUS accounting message before the message is declared as failed.

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

Default: Disabled

**timeout timeout_duration**

Specifies the duration to wait for a response from a RADIUS server before retransmitting a request.

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

Default: 3

**Usage Guidelines**

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

**Examples**

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

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

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

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

Examples
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

**Command Modes**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
radius accounting algorithm { first-n n | first-server [fallback] | 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 accounting 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 [fallback]**

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

**fallback**: This algorithm is an extension of the existing "first-server" algorithm. This algorithm specifies that the context must send accounting data to the RADIUS server with the highest configured priority. When the
server is unreachable, accounting data is sent to the server with the next highest configured priority. If a higher priority server recovers back, the accounting requests of existing sessions and new sessions are sent to the newly recovered server.

This new algorithm behaves similar to “first-server” algorithm, i.e. the accounting data is sent to the highest priority RADIUS/mediation server at any point of time.

If the highest priority server is not reachable, accounting data is sent to the next highest priority server. The difference between "first-server" and "first-server fallback" is that, with the new algorithm, if a higher priority server recovers, all new RADIUS requests of existing sessions and new accounting sessions are sent to the newly available higher priority server. In the case of "first-server" algorithm, the accounting requests of existing sessions continued to be sent to the same server to which the previous accounting requests of those sessions were sent.

The following are the two scenarios during which the requests might be sent to lower priority servers even though a higher priority server is available:

- When `radius max-outstanding` command or `max-rate` is configured, there are chances that the generated requests might be queued and waiting to be sent when bandwidth is available. If a higher priority server recovers, the queued requests will not be switched to the newly available higher priority server.

- When a higher priority server becomes reachable, all existing requests, which are being retried to a lower priority server, will not be switched to the newly available higher priority RADIUS server.

**round-robin**

Specifies that the context must load balance sending accounting data among all of the defined RADIUS accounting 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.

In releases to prior to 17, for subscribers with IMSI containing hexadecimal characters the round robin algorithm fails causing the messages to be forwarded to a single RADIUS server all the time. This algorithm works only for decimal based IMSI addresses. In 17 and later releases, support is extended to hexadecimal based IMSI addresses. That is, IMSI based round robin would be done for subscribers with hexadecimal based IMSI addresses.

**Usage Guidelines**

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

**Examples**

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

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

Entering the above command sequence results in the following prompt:

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

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

Examples
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

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

Entering the above command sequence results in the following prompt:
{context_name}host_name(config-aaa-group)#

Syntax Description
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 to the GGSN Service Configuration Mode Commands chapter.

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

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

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

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

**Product**
HA

**Privilege**
Security Administrator, Administrator

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

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-aaa-group)#

**Syntax Description**
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 Guidelines**
Use this command to configure the AAA accounting behavior for an HA session.
Examples

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

Command Modes

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

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-aaa-group)#

Syntax Description

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

no radius accounting interim volume

no

Disables RADIUS interim accounting.

interval interim_interval

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

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

downlink bytes uplink bytes: Specifies the downlink to uplink volume limit, in bytes, for RADIUS Interim accounting. bytes must be an integer from 100000 through 4000000000.

total bytes: Specifies the total volume limit, in bytes, for RADIUS interim accounting. bytes must be an integer from 100000 through 4000000000.

uplink bytes downlink bytes: Specifies the uplink to downlink volume limit, in bytes, for RADIUS interim accounting. bytes must be an integer from 100000 through 4000000000.
Usage Guidelines

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.

Examples

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

**Command Modes**

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

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

Entering the above command sequence results in the following prompt:

```
{context_name}host_name{config-aaa-group}#
```

**Syntax Description**

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

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

- **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 Guidelines**

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.

**Examples**

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

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

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

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

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

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-aaa-group)#
```

**Syntax Description**

```
radius accounting keepalive { calling-station-id id | consecutive-response consecutive_responses | framed-ip-address ipv4/ipv6_address | interval seconds | retries number | timeout seconds | username user_name }

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

no radius accounting keepalive framed-ip-address

no

Removes the specified configuration.

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 alphanumeric string of size 1 to 15 characters.

Default: 000000000000000

consecutive-response consecutive_responses

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

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

Default: 1
The keepalive request is tried every 0.5 seconds (non-configurable) to mark the server as up.

Important

In this case (for keepalive approach) "radius accounting deadtime" parameter is not applicable.

framed-ip-address ipv4/ipv6_address

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

ipv4/ipv6_address must be specified using IPv4 dotted-decimal notation or IPv6 colon-separated hexadecimal notation.

Notes:

• The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In Release 19, a combination of IPv4 and IPv6 addresses is not supported.

• The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.

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 timeout_duration

Configures the time interval between each keepalive access request retries.

timeout_duration must be an integer from 1 through 30.

Default: 3 seconds

username user_name

Configures the user name to be used for authentication.

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

Default: Test-Username

Usage Guidelines

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

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

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

**Product**
PDIF

**Privilege**
Administrator, Security Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

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

default radius accounting pdif trigger-policy

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 Guidelines**

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

**Examples**

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

*default radius accounting pdif trigger-policy*
radius accounting rp

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

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

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

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-aaa-group)#
```

**Syntax Description**
```
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 the specified configuration.

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

**handoff-stop { immediate | 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.

Default: **wait-active-stop**
**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 }**

*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.

Default: **active-handoff**: Disabled

---

**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.

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

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

```bash
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:

```bash
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

Command Modes

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

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius [mediation-device] accounting server ipv4/ipv6_address [encrypted] [key value] [acct-on { disable | enable }] [acct-off { disable | enable }] [admin-status { disable | enable }] [max max_messages] [max-rate max_value] [oldports] [port port_number] [priority priority] [type { mediation-device | standard }] [-noconfirm]

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.

ipv4/ipv6_address

Specifies the IP address of the accounting server. ip_address must be specified using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. 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.

Notes:

- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In Release 19, a combination of IPv4 and IPv6 addresses is not supported.
• The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>The same RADIUS server IP address and port can be configured in multiple RADIUS server groups within a context.</td>
</tr>
</tbody>
</table>

**port port_number**

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

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>The same RADIUS server IP address and port can be configured in multiple RADIUS server groups within a context.</td>
</tr>
</tbody>
</table>

```
[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.

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

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

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 {disable | enable}
```

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

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.

In releases prior to 18.0, whenever a chassis boots up or when a new RADIUS accounting server or RADIUS mediation-device accounting server is configured with Acct-On configuration enabled, the state of the RADIUS server in all the AAA manager instances was initialized to "Waiting-for-response-to-Accounting-On". The Acct-On transmission and retries are processed by the Admin-AAAmgr.

When the Acct-On transaction is complete (i.e., when a response for Accounting-On message is received or when Accounting-On message is retried and timed-out), Admin-AAAmgr changes the state of the RADIUS accounting server to Active in all the AAA manager instances. During the period when the state of the server...
is in "Waiting-for-response-to-Accounting-On", any new RADIUS accounting messages which are generated as part of a new call will not be transmitted towards the RADIUS accounting server but it will be queued. Only when the state changes to Active, these queued up messages will be transmitted to the server.

During ICSR, if the interface of the radius nas-ip address is srp-activated, then in the standby chassis, the sockets for the nas-ip will not be created. The current behavior is that if the interface is srp-activated Accounting-On transaction will not happen at ICSR standby node and the state of the RADIUS server in all the AAAmgr instances will be shown as "Waiting-for-response-to-Accounting-On" till the standby node becomes Active.

In 18.0 and later releases, whenever the chassis boots up or when a new RADIUS accounting server or RADIUS mediation-device accounting server is configured with Acct-On configuration enabled, the state of the RADIUS server will be set to Active for all the non-Admin-AAAmgr instances and will be set to "Waiting-for-response-to-Accounting-On" for only Admin-AAAmgr instance. The Accounting-On transaction logic still holds good from Admin-AAAmgr perspective. However, when any new RADIUS accounting messages are generated even before the state changes to Active in Admin-AAAmgr, these newly generated RADIUS accounting messages will not be queued at the server level and will be transmitted to the RADIUS server immediately.

During ICSR, even if the interface of radius nas-ip address is srp-activated, the state of the RADIUS accounting server will be set to Active in all non-Admin-AAAmgr instances and will be set to "Waiting-for-response-to-Accounting-On" in Admin-AAAmgr instance.

```plaintext
acct-off { disable | 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.

Default: enable

```plaintext
max max_messages
```

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

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

Default: 0

```plaintext
max-rate max_value
```

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

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

Default: 0 (disabled)

```plaintext
oldports
```

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

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.

Default: 1000

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

**mediation-device**: Obsolete keyword.

Specifies the type of AAA transactions to use to communicate with this RADIUS server.

**standard**: Use standard AAA transactions.

Default: **standard**

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

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 Guidelines**

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

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

**Examples**

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

```
radius mediation-device accounting server 10.2.3.4 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

Command Modes

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

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius algorithm { first-server | round-robin }

default radius algorithm

default

Configures the default setting.

Default: first-server

first-server

Authentication data is sent to the first available authentication 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 authentication 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 Guidelines

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

Examples

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

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 products used in CDMA deployments

Privilege
Security Administrator, Administrator

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

Entering the above command sequence results in the following prompt:

<context_name>host_name(config-aaa-group)#

Syntax Description
| no | radius allow { authentication-down | accounting-down } |

no
Specifies that the specified option is to be disabled.

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

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

Usage Guidelines
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.

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

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

```
radius allow accounting-down
```
radius attribute

This command configures the system's RADIUS identification parameters.

Product All

Privilege Security Administrator, Administrator

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

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-aaa-group)#

Syntax Description

radius attribute \{ accounting accounting_attribute \| authentication authentication_attribute \| nas-identifier nas_id \| nas-ip-address address primary_ipv4/ipv6_address \| backup secondary_ipv4/ipv6_address \| nexthop-forwarding-address nexthop_ipv4/ipv6_address \| mpls-label input in_label_value \| output out_label_value1 \| out_label_value2 \| vlan vlan_id \}\}

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

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

no

Removes or disables the specified configuration.

default

Configures the default setting(s).

accounting accounting_attribute

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

- 3gpp-cg-address
- 3gpp-charging-characteristics
- 3gpp-charging-id
- 3gpp-ggsn-address
- 3gpp-ggsn-mcc-mnc
• 3gpp-gprs-qos-negotiated-profile
• 3gpp-imeisv
• 3gpp-imsi-mcc-mnc
• 3gpp-ms-timezone
• 3gpp-nsapi
• 3gpp-pdp-type
• 3gpp-rat-type
• 3gpp-select-mode
• 3gpp-session-stopindicator
• 3gpp-sgsn-address
• 3gpp-sgsn-mcc-mnc
• 3gpp-user-location-info
• acct-authentic
• acct-delay-time
• acct-input-octets
• acct-input-packets
• acct-output-octets
• acct-output-packets
• acct-session-id
• acct-session-time
• acct-statustype
• called-station-id
• calling-station-id
• class
• event-timestamp
• framed-ip-address
• framed-ipv6-prefix

In Releases 19.4 and beyond, this attribute option will also include delegated-ipv6-prefix to support DHCPv6 Prefix Delegation via RADIUS server.
• imsi
• nas-identifier
• nas-ip-address
• nas-port-id
• nas-port-type
• service-type
• username

By default, all of the attributes are enabled except for nas-port-id attribute.

**authentication authentication_attribute**

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

• 3gpp-cg-address
• 3gpp-charging-characteristics
• 3gpp-ggsn-address
• 3gpp-ggsn-mcc-mnc
• 3gpp-gprs-qos-negotiated-profile
• 3gpp-imeisv
• 3gpp-imsi-mcc-mnc
• 3gpp-ms-timezone
• 3gpp-nsapi
• 3gpp-pdp-type
• 3gpp-rat-type
• 3gpp-select-mode
• 3gpp-sgsn-address
• 3gpp-sgsn-mcc-mnc
• 3gpp-user-location-info
• called-station-id
• calling-station-id
• chap-challenge
• framed-ipaddress
• framed-ipv6-prefix
• imsi
• nas-identifier
• nas-ip-address
• nas-port-id
• nas-port-type
• service-type
• username
By default, all of the attributes are enabled except for nas-port-id attribute.

**nas-identifier nas_id**

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

**nas-ip-address address primary_ipv4/ipv6_address**

Specifies the AAA interface IP address(es) used to identify the system. Up to two addresses can be configured. `primary_ipv4/ipv6_address`: The IP address of the primary interface to use in the current context. This must be specified using the IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Notes:**
- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In this release, a combination of IPv4 and IPv6 addresses is not supported.
- When a RADIUS server is configured in non-default AAA group without nas-ip, the NAS IP is taken from the default group. In this scenario, the IP address should be of the same transport type.
- The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.
- It is recommended that the primary and secondary server IP addresses should be of the same transport type.

**backup secondary_ipv4/ipv6_address**

`backup`: The IP address of the secondary interface to use in the current context. This must be specified using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Notes:**
- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In this release, a combination of IPv4 and IPv6 addresses is not supported.
- When a RADIUS server is configured in non-default AAA group without nas-ip, the NAS IP is taken from the default group. In this scenario, the IP address should be of the same transport type.
- The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.
- It is recommended that the primary and secondary server IP addresses should be of the same transport type.

**nexthop-forwarding-address nexthop_ipv4/ipv6_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_ipv4/ipv6_address` must be specified using IPv4 dotted-decimal notation.
Notes:

• The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In Release 19, a combination of IPv4 and IPv6 addresses is not supported.

• The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.

Important

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 `nexthop_address` keyword and `aaa-large configuration` is enabled at Global Configuration level.

Usage Guidelines

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.

Examples

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

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

This command configures RADIUS authentication related parameters.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

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

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

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

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

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

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

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

```plaintext
radius authenticate null-username
```
radius authenticator-validation

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

Product

All

Privilege

Security Administrator, Administrator

Command Modes

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

Entering the above command sequence results in the following prompt:

/context_name/host_name(config-aaa-group)#

Syntax Description

| default | no | radius authenticator-validation

no

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

Usage Guidelines

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

Examples

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

no radius authenticator-validation

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

radius authenticator-validation
radius charging

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

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

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

**Syntax Description**

```
radius charging { deadtime dead_time | detect-dead-server { consecutive-failures consecutive_failures_count | response-timeout response_timeout_duration } | max-outstanding max_messages | max-retries max_retries | max-transmissions max_transmissions | timeout idle_seconds } default radius charging { deadtime | detect-dead-server | max-outstanding | max-retries | max-transmissions | timeout } no radius charging { detect-dead-server | max-transmissions | timeout }
```

- **no**
  Removes the specified configuration.
  
- **default**
  Configures the default setting for the specified keyword.
  
- **deadtime dead_time**
  Specifies the number of minutes to wait before attempting to communicate with a server that has been marked as unreachable.
  
  *dead_time* must be an integer from 0 through 65535.
  
  Default: 10
  
- **detect-dead-server { consecutive-failures consecutive_failures_count | response-timeout response_timeout_duration }**
  
  - **consecutive-failures consecutive_failures_count**: Specifies the number of consecutive failures, for each AAA Manager, before a server is marked as unreachable.
consecutive_failures_count must be an integer from 1 through 1000.
Default: 4

response-timeout response_timeout_duration: 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.
response_timeout_duration must be an integer from 1 through 65535.

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

max-retries max_retries
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.
max_retries must be an integer from 0 through 65535.
Default: 5

max-transmissions max_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 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.
max_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 Guidelines
Use this command to manage the basic Charging Service RADIUS options according to the RADIUS server used for the context.

Examples
The following command configures the AAA server to be marked as unreachable when the consecutive failure count exceeds 6:
radius charging detect-dead-server consecutive-failures 6
The following command sets the timeout value to 300 seconds to wait for a response from RADIUS server before resending the messages:

```
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

**Command Modes**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

\[\text{context_name}\]host_name(config-aaa-group)#

**Syntax Description**

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

**first-n n**

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.

Default: 1 (Disabled)

**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 Guidelines

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

Examples

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

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

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

Product
All

Privilege
Security Administrator, Administrator

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

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-aaa-group)#

Syntax Description

radius charging accounting server ipv4/ipv6_address | encrypted | key value | max max_messages | | oldports | | port port_number | | priority priority | | admin-status { enable | disable } | | -noconfirm |

no

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

ipv4/ipv6_address

Specifies the IP address of the accounting server. ip_address must be specified using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

Notes:

- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In Release 19, a combination of IPv4 and IPv6 addresses is not supported.

- The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.

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

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

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

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

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

**priority priority**
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.
Default: 1000

**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 Guidelines**
This command is used to configure the RADIUS charging accounting server(s) with which the system is to communicate for ACS Prepaid Accounting requests.
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.
Examples

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

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

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

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

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

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

**default**
Configs 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 Guidelines**
Use this command to configure the context's RADIUS server selection algorithm for ACS to ensure proper load distribution amongst the available servers.

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

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

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**

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

`configure > context context_name > aaa group group_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
radius charging server ipv4/ipv6_address | encrypted | key value | max max_messages | | oldports | |
port port_number | | priority priority | | admin-status { enable | disable } | | -noconfirm |
no radius charging server ipv4/ipv6_address | oldports | port port_number |
```

**no**

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

**ipv4/ipv6_address**

Specifies the IP address of the server. `ipv4/ipv6_address` must be specified using IPv4 dotted-decimal notation or IPv6 colon-separated hexadecimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

**Notes:**

- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In Release 19, a combination of IPv4 and IPv6 addresses is not supported.

- The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.

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

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

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 max_messages**

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

Default: 256

**oldports**

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

**port port_number**

Specifies the port number to use for communications.

port_number must be an integer from 1 through 65535.

Default: 1812

**priority priority**

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.

Default: 1000

**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 Guidelines**

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

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

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

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

Product
All

Privilege
Security Administrator, Administrator

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

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

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

Syntax Description
radius ip vrf vrf_name
no radius ip vrf

no
Disables the configured IP Virtual Routing and Forwarding (VRF) context instance and removes the association between the VRF context instance and the AAA group instance (NAS-IP).
By default this command is disabled, which means the NAS-IP being used is assumed a non-VRF IP and specific AAA group does not have any VRF association.

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

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

Usage Guidelines
Use this command to associate/disassociate a pre-configured VRF context for a feature such as BGP/MPLS VPN or GRE, and IPSec tunneling which needs VRF support for RADIUS communication.
By default the VRF is NULL, which means that AAA group (NAS-IP) is associated with global routing table and NAS-IP being used is assumed a non-VRF IP.

This IP VRF feature can be applied to RADIUS communication, which associates the VRF with the AAA group. This command must be configured whenever a VRF IP is used as a NAS-IP in the AAA group or at the Context level for the "default" AAA group.

This is a required configuration as VRF IPs may be overlapping hence AAA needs to know which VRF the configured NAS-IP belongs to. By this support different VRF-based subscribers can communicate with different RADIUS servers using the same, overlapping NAS-IP address, if required across different AAA groups.

**Examples**

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

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

This command configures the RADIUS keepalive authentication parameters.

**Product**
All

**Privilege**
Security Administrator, Administrator

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

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

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

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 alphanumeric string of size 1 to 15 characters.

Default: 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 10.

Default: 1

---

**Important**
The keepalive request is tried every 0.5 seconds (non-configurable) to mark the server as up.
In this case (for keepalive approach) "radius deadtime" parameter is not applicable.

**encrypted password**

Specifies encrypting the password.

In 12.1 and earlier releases, the *password* must be an alphanumeric string of 1 through 63 characters.

In StarOS 12.2 and later releases, *password* must be an alphanumeric string of 1 through 132 characters.

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 alphanumeric string of 1 through 63 characters.

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 timeout_duration**

Specifies the time interval between keepalive access request retries.

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

Default: 3 seconds

**username user_name**

Specifies the user name to be used for authentication.

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

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

Examples
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 command.
radius probe-interval

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

Product
All

Privilege
Security Administrator, Administrator

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

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

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

Syntax Description
radius probe-interval seconds
default radius probe-interval

default
Configures the default setting.

seconds
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.
Default: 60

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

Examples
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

**Command Modes**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

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

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-aaa-group)#
```

**Syntax Description**

```
radius probe-max-retries retries
default radius probe-max-retries
```

**default**
Configures the default setting.

**retries**
Specifies the number of retries for RADIUS authentication probe response before the authentication is declared as failed.

**Usage Guidelines**

Use this command with Interchassis Session Recovery (ICSR) to set the number of attempts to send RADIUS authentication probe without a response before the authentication is declared as failed.

**Examples**

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 Interchassis Session Recovery (ICSR) to wait for a response for RADIUS authentication probes.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

`configure > context context_name > aaa group group_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
radius probe-timeout idle_seconds
default radius probe-timeout
```

- **default**
  Configures the default setting.

- **idle_seconds**
  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.
  Default: 3

**Usage Guidelines**

Use this command to set the time duration for ICSR, to wait for a response before re-sending the RADIUS authentication probe to the RADIUS server.

**Examples**

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

**Command Modes**

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

Entering the above command sequence results in the following prompt:

```
(config-aaa-group)#
```

**Syntax Description**

- `radius server ipv4/ipv6_address [encrypted] [key value | admin-status {disable | enable}] [max max_messages] [max-rate max_value] [oldports] [port port_number] [priority priority] [probe | no-probe] [probe-username user_name | probe-password {encrypted | password} password] [type {mediation-device | standard}] [-noconfirm]`

- `no radius server ipv4/ipv6_address [oldports] [port port_number]`

- `no`

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

**ipv4/ipv6_address**

Specifies the IP address of the server.

*ipv4/ipv6_address*: Must be specified using IPv4 dotted-decimal notation or IPv6 colon-separated hexadecimal notation. 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.

**Notes:**

- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In Release 19, a combination of IPv4 and IPv6 addresses is not supported.

- The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.
The same RADIUS server IP address and port can be configured in multiple RADIUS server groups within a context.

```
port port_number
```

Specifies the port number of the server.

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

The 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.

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

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

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.

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

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.

```
max max_messages
```

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

```
max_messages must be an integer from 0 through 4000.
Default: 256
```

```
max-rate max_value
```

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

```
max_value must be an integer from 0 through 1000.
Default: 0 (disabled)
```
oldports
Sets the UDP communication port to the old default for RADIUS communications to 1645.

priority priority
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.

Default: 1000

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 user_name
The user name sent to the RADIUS server to authenticate probe messages. user_name must be an alphanumeric string of 1 through 127 characters.

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 alphanumeric string of 1 through 63 characters.

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 Cisco representative for licensing information.

standard: Specifies standard AAA transactions. (Default)

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

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

**Examples**

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

```
radius server 10.2.3.4 key sharedKey212 port 1024 max 127
radius server 10.2.3.4 encrypted key scrambledKey234 oldports priority 10
```
radius trigger

This command enables specific RADIUS triggers.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] radius trigger { ms-timezone-change | qos-change | rai-change | rat-change | serving-node-change | uli-change }
default radius trigger
```

- **no**
  Disables specified RADIUS trigger.

- **default**
  Configures the default setting.
  Default: All RADIUS triggers are enabled.

- **ms-timezone-change**
  Specifies to enable RADIUS trigger for MS time zone change.

- **qos-change**
  Specifies to enable RADIUS trigger for Quality of Service change.

- **rai-change**
  Specifies to enable RADIUS trigger for Routing Area Information change.
rat-change
Specifies to enable RADIUS trigger for Radio Access Technology change.

serving-node-change
Specifies to enable RADIUS trigger for Serving Node change.

uli-change
Specifies to enable RADIUS trigger for User Location Information change.

Usage Guidelines
Use this command to enable RADIUS triggers.

Examples
The following command enables RADIUS trigger for RAT change:
radius trigger rat-change
radius trigger
AAL2 Node Configuration Mode Commands

**Important** In Release 20.0, HNBGW is not supported. Commands in this configuration mode must not be used in Release 20.0. For more information, contact your Cisco account representative.

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.

**Command Modes**

Exec > Global Configuration > Context Configuration > ALCAP Service Configuration > AAL2 Node Configuration

```
configure > context context_name > alcap-service service_name > aal2-node node_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aal2-node-node_name) #
```

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

- aal2-path-id, page 116
- end, page 118
- exit, page 119
- point-code, page 120
**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

**Command Modes**

Exec > Global Configuration > Context Configuration > ALCAP Service Configuration > AAL2 Node Configuration

```plaintext
configure > context context_name > alcap-service service_name > aal2-node node_name
```

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-aal2-node-node_name)#
```

**Syntax Description**

```
[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 4294967295.

**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 block 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 Guidelines

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.

Examples

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.

`no aal2-path-id 6 block`
**end**

Exits the current mode and returns to the Exec Mode.

<table>
<thead>
<tr>
<th><strong>Product</strong></th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privilege</strong></td>
<td>Security Administrator, Administrator</td>
</tr>
<tr>
<td><strong>Syntax Description</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Usage Guidelines</strong></td>
<td>Change the mode back to the Exec mode.</td>
</tr>
</tbody>
</table>
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax Description
exit

Usage Guidelines
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

Command Modes

Exec > Global Configuration > Context Configuration > ALCAP Service Configuration > AAL2 Node Configuration

configure > context context_name > alcap-service service_name > aal2-node node_name

Entering the above command sequence results in the following prompt:

/context_name/host_name(config-aal2-node-node_name) #

Syntax Description

[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.

point_code: 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 Guidelines

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 16 point codes for adjacent AAL2 nodes can be configured in one ALCAP service.
Examples

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
```
point-code

AAL2 Node Configuration Mode Commands
Accounting Policy Configuration Mode

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.

**Command Modes**

Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-accounting-policy)#

**Important**

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

- accounting-event-trigger, page 125
- accounting-keys, page 127
- accounting-level, page 129
- accounting-mode, page 132
- apn-name-to-be-included, page 133
- attribute, page 134
- cc, page 135
- end, page 138
- exit, page 139
- max-containers, page 140
- operator-string, page 142
- rf, page 143
• service-context-id, page 145
• session, page 146
• trigger-type, page 148
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
- SAEGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

`configure > context context_name > policy accounting policy_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-accounting-policy)#`

**Syntax Description**

`accounting-event-trigger { cgi-sai-change | ecgi-change | flow-information-change | interim-timeout | location-change | rai-change | tai-change } action { interim | stop-start }`

- **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.

- **cgi-sai-change**
  Specifies that the action is initiated upon indication of a Cell Global Identification-Service Area Identification (CGI-SAI) change.

- **ecgi-change**
  Specifies that the action is initiated upon indication of an E-UTRAN Cell Global Identifier (ECGI) change.
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 a location change.

rai-change
Specifies that the action is initiated upon indication of an Routing Area Identifier (RAI) change.

tai-change
Specifies that the action is initiated upon indication of a Tracking Area Identity (TAI) change.

action { interim | stop-start }
Default: interim
Specifies the action initiated upon the occurrence of an event.
interim: Specifies that an interim ACR (Accounting Request) is sent.
stop-start: Specifies that a Stop-Start ACR is sent.

Usage Guidelines
Use this command to configure that action taken upon the occurrence of an accounting event trigger.

Examples
The following command configures the policy to send a Stop-Start ACR upon indication of an interim timeout:
accounting-event-trigger interim-timeout action stop-start
accounting-keys

Aggregates the accounting information, using the configurable keys (QCI) along with default keys.

### Product
- HSGW
- P-GW
- S-GW
- SAEGW

### Privilege
Administrator

### Command Modes
- Exec > Global Configuration > Context Configuration > Accounting Policy Configuration
- configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-accounting-policy)#
```

### Syntax Description
- **accounting-keys qci**
- **default accounting-keys**
  
  **default**
  Aggregates the accounting information using QoS Class Identifier (QCI) as the additional key.
  
  **qci**
  Aggregates the accounting information using QCI as the additional key.

### Usage Guidelines
Use this command to aggregate the accounting information using the configurable keys (QCI) along with default keys.

In Service Data Flow (SDF) level accounting, buckets are created and maintained using the Reporting-Level AVP value present in Gx message. The following are the accounting keys currently supported:

- Rating-group
- Rating-group and Service-Identifier
- Rating-group and QCI
- Rating-group, Service-Identifier, and QCI
Examples

The following command aggregates the accounting information using QCI as the additional key:

```text
accounting-keys qci
```
accounting-level

Configures the type of accounting performed by this profile.

**Product**

HSGW
P-GW
S-GW
SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-accounting-policy)#

**Syntax Description**

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 Evolved Packet System (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/S-GW
• Address of the P-GW (if available), one or more instances

**pdn**

Specifies that PDN-based accounting is to be used for this accounting profile. 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/S-GW
• Address of the P-GW (if available), one or more instances

**pdn-qci**

Specifies that PDN-QCI accounting is to be used for this accounting profile. 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/S-GW
• Address of the P-GW (if available), one or more instances

**qci**

Specifies that QCI-based accounting is to be used for this accounting profile. 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/S-GW
• Address of the P-GW (if available), one or more instances

**sdf**

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

• User Equipment information if available (ESN/MEID)
• Address of HSGW/S-GW
• Address of the P-GW (if available), one or more instances

**Usage Guidelines**

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

**Examples**

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
- SAEGW

Privilege
- Administrator

Command Modes
- Exec > Global Configuration > Context Configuration > Accounting Policy Configuration
- configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-accounting-policy)#

Syntax Description
- 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 Guidelines
Use this command to set the accounting mode for this profile.
**apn-name-to-be-included**

This command configures whether the virtual or real Access Point Name (APN) is sent in Rf accounting message.

**Product**

GGSN
P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-accounting-policy)#
```

**Syntax Description**

`apn-name-to-be-included { gn | virtual }

default apn-name-to-be-included`

- **default**
  
  Configures this command with the default setting.
  
  Default: `gn`

- **gn**

  Sends the Gn APN name in the Rf accounting messages.

- **virtual**

  Sends the virtual APN name, if configured in the APN Configuration Mode, in the Rf accounting messages.

**Usage Guidelines**

Use this command to configure the APN name to be included in Rf accounting messages. Virtual APN name can be set to be sent in Rf accounting messages if it is configured in the APN Configuration Mode.

**Examples**

The following command sets the virtual APN name to be sent in Rf accounting message:

```
apn-name-to-be-included virtual
```
**attribute**

This command configures the attributes to be reported in Rf accounting.

**Product**

P-GW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

```
configure > context context_name > policy accounting policy_name
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-accounting-policy)#
```

**Syntax Description**

```
| default | no | attribute csg
```

- `[default | no]

Specifies to disable reporting of attributes in Rf accounting.

- `csg`

Specifies to enable reporting of Closed Subscriber Group (CSG) related IEs received during the initial attach (Create Session Request) for Rf accounting purpose.

**Usage Guidelines**

Use this command to enable or disable the reporting of attributes received during the initial attach (Create Session Request) for Rf billing purpose.
**CC**

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

**Product**
- ePDG
- GGSN
- HSGW
- P-GW
- S-GW
- SAEGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

```bash
configure > context context_name > policy accounting policy_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-accounting-policy)#
```

**Syntax Description**

```
cr profile index { buckets num | interval seconds | sdf-interval seconds | sdf-volume { downlink octets { uplink octets | total octets | uplink octets { downlink octets } } | serving-nodes num | 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 | sdf-interval | sdf-volume | serving-nodes | tariff | volume }
default
```

**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. If an accounting policy is not configured, this value is 4. GTPP accounting will use the default value if the configured value is beyond 4.
In 12.1 and earlier releases, *num* must be an integer value from 1 through 4.
In release 12.2, *num* must be an integer value from 1 through 10.
In 12.3 and later releases, *num* must be an integer value from 1 through 20.

**Important**
Please note that the maximum value for the CC profile buckets is extended to support up to 10 for Diameter Rf accounting only. However, in the case of GTPP accounting, this CLI command allows configuring only up to 4 buckets.

**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 through 40000000.

**sdf-interval seconds**
Default: disabled
Specifies a time interval for closing the charging record for a specific flow if the minimum volume thresholds are satisfied. *seconds* must be an integer value from 60 through 40000000.

**sdf-volume { downlink octets | uplink octets } | total octets | uplink octets | downlink octets }**
Specifies octet volume thresholds for the generation of interim CDRs for a specific flow.
**downlink octets**: Sets the threshold limit for the number of downlink octets that must be reached before the charging record for a specific flow is closed. *octets* must be an integer value from 100000 through 4000000000.
**total octets**: Sets the threshold limit for the total number of octets that must be reached before the charging record for a specific flow is closed. *octets* must be an integer value from 100000 through 4000000000.
**uplink octets**: Sets the threshold limit for the number of uplink octets that must be reached before the charging record for a specific flow is closed. *octets* must be an integer value from 100000 through 4000000000.

**serving-nodes num**
Default: 4
Specifies the number of serving node changes (inter-serving node switchovers) after which the interim CDR is generated. In P-GW and S-GW, a partial record needs to be generated whenever there is a serving node
address list overflow. Serving node is added to the CDR list during handover scenarios. \textit{num} must be an integer value from 1 through 15. If an accounting policy is not configured, this value is 4.

\textbf{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.

\textit{time1 min hrs}: Specifies the first time-of-day value used to close the current container in the charging record. \textit{min} must be an integer value from 0 through 59. \textit{hrs} must be an integer value from 0 through 23.

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

\textbf{volume \{ downlink octets \uplink octets \} total octets \uplink octets \{ downlink octets \}}

Specifies octet volume thresholds for the generation of interim CDRs.

\textit{downlink octets}: Sets the threshold limit for the number of downlink octets that must be reached before the charging record is closed.

In 12.1 and earlier releases, the downlink \textit{octets} must be an integer value from 100000 to 1345294336.

In 12.2 and later releases, the downlink \textit{octets} must be an integer value from 100000 to 4000000000.

\textit{total octets}: Sets the threshold limit for the total number of octets that must be reached before the charging record is closed.

In 12.1 and earlier releases, the total\textit{octets} must be an integer value from 100000 to 4000000000.

In 12.2 and later releases, the total \textit{octets} must be an integer value from 100000 to 4000000000.

\textit{uplink octets}: Sets the threshold limit for the number of uplink octets that must be reached before the charging record is closed.

In 12.1 and earlier releases, the uplink \textit{octets} must be an integer value from 100000 to 4000000000.

In 12.2 and later releases, the uplink \textit{octets} must be an integer value from 100000 to 4000000000.

\textbf{Usage Guidelines}

Use this command to set charging characteristics that directly affect the CDR generation on the HSGW, P-GW, or S-GW.

\textbf{Examples}

The following command creates a hot billing profile with a total octet volume threshold set to 500000:

\texttt{cc profile 1 volume total 500000}
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

end

Usage Guidelines

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 Description**
- exit

**Usage Guidelines**
Use this command to return to the parent configuration mode.
max-containers

Control the number of containers in an ACR message.

**Product**

- GGSN
- HSGW
- P-GW
- S-GW
- SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-accounting-policy)#
```

**Syntax Description**

```
max-containers { containers | fill-buffer }
default max-containers

default

Cache containers until buffer is filled.

containers

System can send any value equal or less than the maximum number of containers selected. The number of containers that can be sent can be dynamically selected by the system, but it should not cross the limit of containers in any message.

containers must be in integer from 1 to 30.

fill-buffer

Cache containers until buffer is filled.

**Usage Guidelines**

Use this command to control the number of containers before an interim ACR message is triggered.
The following command sets a maximum of 20 containers in an ACR message:

```
max-containers 20
```
**operator-string**

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

**Product**

- HSGW
- P-GW
- S-GW
- SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

```
configure > context context_name > policy accounting policy_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-accounting-policy)#
```

**Syntax Description**

- **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 alphanumeric characters.

**Usage Guidelines**

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

**Examples**

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

```
operator-string pgw_local
```
This command controls the reporting of subscriber traffic data for Rating Groups (RGs) based on the generation of Interim Record (IR).

**Product**
- GGSN
- HSGW
- P-GW
- S-GW
- SAEGW

**Privilege**
- Administrator

**Command Modes**
```
Exec > Global Configuration > Context Configuration > Accounting Policy Configuration
```
```
configure > context context_name > policy accounting policy_name
```

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

**Syntax Description**
```
rf report-all-active-rgs
{ default | no } rf report-all-active-rgs
```

**default | no**
The default behavior is to disable traffic data reporting in Service Data Container (SDC) for all active Rating Groups (RGs) whenever an interim is sent.

**report-all-active-rgs**
This keyword enables to report the traffic data in the SDC for all the active RGs whenever an IR is sent. By default, this feature is enabled.

**Usage Guidelines**
There are several change conditions where a partial Service Data Container (SDC) is not cut for a particular RG but ACR-Interim is generated due to maximum change conditions. There are many triggers like time limit, volume limit, etc., that will lead to maximum change condition. Because of this some RGs SDC may not be generated for a longer period of time.

In releases prior to 18.0, when a Maximum Change Condition event was triggered, only those RGs that have hit one of the Change Conditions that require a caching of data as opposed to cutting an IR, used to have their
data in the generated IR. In 18.0 and later releases, when the Maximum Change Condition happens, the current Rf implementation is changed to make sure all RGs that have not been cached have a snapshot of their usage taken.

This CLI configuration will enable Rf to take a snapshot of all the active Rating Groups (RGs) whenever an Interim Record (IR) is generated. That means, the Rf will be enabled to report the subscriber traffic data in SDC whenever an IR is generated.

This feature is introduced mainly to ensure that the snapshot is available for all active RGs including the default bearer's RG so that all the traffic data is accounted during the billing cycle.

**Examples**

The following command specifies to report the traffic data for all active RGs when an IR is sent:

```
rf report-all-active-rgs
```
service-context-id

Configures the value to be sent in the Service-Context-Id AVP, which defines the context in which Rf is used.

**Product**

GGSN
HSGW
P-GW
S-GW
SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-accounting-policy)#

**Syntax Description**

service-context-id service_context_id
default service-context-id

default

Configures this command with the default setting. Currently, the default value is encoded based on the dictionary wherever applicable; when not applicable, it is not encoded.

service_context_id

Specifies the service context as an alphanumeric string of 1 through 63 characters that can contain punctuation characters.

**Usage Guidelines**

If Service-Context-Id is applicable and configured using this command, it will be sent in the AVP Service-Context-Id in the Rf ACR message.

**Examples**

The following command specifies the value version@customer.com to be sent in the Service-Context-Id AVP in the Rf ACR message:

service-context-id version@customer.com
session

This command controls the behavior of whether to send or suppress the ACR-Interim records when the UE is idle.

Product P-GW

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:

<context_name>host_name(config-accounting-policy)#

Syntax Description | default | no | session idle-mode suppress-interim

default

The default behavior is to send accounting interim records even when the UE is in idle state and when there is no data to report.

no

Specifies to send the accounting interim records even when the UE is in idle state and when there is no data to report.

suppress-interim

Suppresses the ACR-I records when there is no data to report or the UE is in idle mode.

Usage Guidelines This CLI configuration is used to control sending of ACR-I records when the UE is in idle mode and when there is no data to report.

In a scenario where there is no data to report, upon configuring the CLI command "session idle-mode suppress-interim", a call is established, AII timer (or any other event for which an Interim needs to be generated) happens, and ACR-I will be suppressed.

When there is data to report, on configuring the CLI command "session idle-mode suppress-interim", a call is established, AII timer (or any other event for which an Interim needs to be generated) happens, and ACR-I will be sent out.
When there is data to report for the previous events, the following behavior is observed:

1. The CLI command "session idle-mode suppress-interim" is configured and a call is established.
2. QoS-Change happens (or any other event for which the container needs to be cached) happens, containers are cached.
3. All timer (or any other event for which an Interim needs to be generated) happens, but there is no data to report with this event.
4. ACR-I will be sent with the previously cached containers (QoS-Change in this case).

**Examples**

The following command suppresses sending of ACR-Interim message when the UE is idle or when there is no data to report:

```bash
session idle-mode suppress-interim
```
trigger-type

This command enables/disables the event triggers for Rf-Gy interaction.

Product

GGSN
HSGW
P-GW
S-GW
SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Accounting Policy Configuration
configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:
{context_name} host_name (config-accounting-policy) #

Syntax Description

trigger-type { gy-sdf-time-limit { cache | immediate } | gy-sdf-unit-limit { cache | immediate } |
gy-sdf-volume-limit { cache | immediate } } +
{ default | no } trigger-type

default
The default behavior is to disable all the configured event triggers. The interims will be dropped if the event triggers are received from Gy.

no
Specifies to disable all the configured event triggers. The interims will be dropped if the event triggers are received from Gy.

gy-sdf-time-limit { cache | immediate }
Enables the SDF time-limit trigger for Rf-Gy interaction.

cache: If this keyword option is configured then upon receipt of time-limit event trigger from Gy, the container record will be cached for reporting in a future transaction.

immediate: If this keyword option is configured then upon receipt of time-limit event trigger from Gy, Rf will send out an interim record immediately.
gy-sdf-unit-limit { cache | immediate }

Enables the SDF unit-limit trigger for Rf-Gy interaction in Assume Positive scenario. Upon configuration of the CLI command `trigger-type gy-sdf-unit-limit { cache | immediate }`, when the session gets terminated during assume-positive case, ACR-Stop is sent with the container-level change-condition as SERVICE-SPECIFIC-UNIT-LIMIT.

gy-sdf-volume-limit { cache | immediate }

Enables the SDF volume-limit trigger for Rf-Gy interaction.

cache: If this keyword option is configured then upon receipt of volume-limit event trigger from Gy, the container record will be cached for reporting in a future transaction.

immediate: If this keyword option is configured then upon receipt of volume-limit event trigger from Gy, Rf will send out an interim record immediately.

+

Indicates that more than one of the keywords can be entered in a single command.

Usage Guidelines

In Release 15.0 when time/volume quota on the Gy interface gets exhausted, Gy will trigger SERVICE_DATA_VOLUME/TIME_LIMIT. Release 16.0 and beyond, this behavior is CLI controlled.

This CLI configuration will either enable PCEF to send an ACR-Interim immediately or cache the container records for reporting in a future transaction. If there is no such configuration for that event-trigger, then the ACR-Interims will be dropped.

When the subscriber disconnects while in Assume Positive mode, then the CLI configuration enables the PCEF to send an ACR-Stop with PS-level change condition "Normal Release" and container level "Service Specific Unit Limit". The presence of the "Service Specific Unit Limit" change condition at the container level indicates to the OFCS that data has gone unreported on Gy. The change-condition at container level is only present if the keyword option gy-sdf-unit-limit is configured.

The gateway provides a configuration option to enable/disable the functionality at the ACR level to control which of the triggers are enabled – Service Specific Unit Limit, Service Data Volume Limit and Service Data Time Limit. The gateway provides configuration options to control the various Rf messages triggered for sync on this feature.

Gy Quota Update - Volume Limit - CLI options are:

- Disabled
- Enabled, container with SDF Volume limit queued and sent at next ACR trigger.
- Enabled, container with SDF Volume limit created and ACR sent immediately with PS info level of Volume Limit

Gy Quota Update – Validity Timer Expires - CLI options are:

- Disabled
- Enabled, container with SDF Time Limit queued and sent at next ACR trigger.
- Enabled, container with SDF Time limit created and ACR sent immediately with PS info level of Time Limit
Examples

The following command specifies to send ACR-Interim message immediately when the time quota on the Gy interface expires:

```
trigger-type gy-sdf-time-limit immediate
```
ACL Configuration Mode Commands

The Access Control List Configuration Mode is used to create and manage IP-based, user access privileges.

**Command Modes**

Exec > Global Configuration > Context Configuration > ACL Configuration

```configure > context context_name > ip access-list acl_name```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Important**

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

- deny/permit (by source IP address masking), page 153
- deny/permit (any), page 156
- deny/permit (by host IP address), page 159
- deny/permit (by source ICMP packets), page 161
- deny/permit (by IP packets), page 165
- deny/permit (by TCP/UDP packets), page 169
- description, page 174
- end, page 175
- exit, page 176
- readdress server, page 177
- redirect context (by IP address masking), page 182
- redirect context (any), page 185
- redirect context (by host IP address), page 188
- redirect context (by source ICMP packets), page 190
- redirect context (by IP packets), page 194
- redirect context (by TCP/UDP packets), page 198
- redirect css delivery-sequence, page 203
- redirect css service (any), page 204
- redirect css service (by host IP address), page 207
- redirect css service (by ICMP packets), page 210
- redirect css service (by IP packets), page 214
- redirect css service (by source IP address masking), page 218
- redirect css service (by TCP/UDP packets), page 221
- redirect css service (for downlink, any), page 226
- redirect css service (for downlink, by host IP address), page 229
- redirect css service (for downlink, by ICMP packets), page 232
- redirect css service (for downlink, by IP packets), page 236
- redirect css service (for downlink, by source IP address masking), page 240
- redirect css service (for downlink, by TCP/UDP packets), page 243
- redirect css service (for uplink, any), page 248
- redirect css service (for uplink, by host IP address), page 251
- redirect css service (for uplink, by ICMP packets), page 254
- redirect css service (for uplink, by IP packets), page 258
- redirect css service (for uplink, by source IP address masking), page 262
- redirect css service (for uplink, by TCP/UDP packets), page 264
- redirect nexthop (by IP address masking), page 269
- redirect nexthop (any), page 272
- redirect nexthop (by host IP address), page 275
- redirect nexthop (by source ICMP packets), page 278
- redirect nexthop (by IP packets), page 282
- redirect nexthop (by TCP/UDP packets), page 286
deny/permit (by source IP address masking)

Filters 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

Command Modes
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

Syntax Description

{ 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 that 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 that 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.

---

**Important**

The logging option is not supported for ACLs applied on SPIO or local contexts.

source_address

The IP address(es) from which the packet originated. IP addresses must be entered in IPv4 dotted-decimal format.

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 Guidelines

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.
The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Examples**

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)

Filters subscriber sessions based on any packet received. This command is also sets the access control list insertion point.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

Syntax Description

{ 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.

Important The logging option is not supported for ACLs applied on SPIO or local contexts.

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

Usage Guidelines 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. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Examples The following commands define two rules with the second logging filtered packets:
  permit any
deny log any
The following sets the insertion point 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)

Filters 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

**Command Modes**

Exec > Global Configuration > Context Configuration > ACL Configuration

`configure > context context_name > ip access-list acl_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax Description**

{ 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.
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 that 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 IPv4 dotted-decimal notation.

**Usage Guidelines**
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.

**Examples**
The following commands define two rules with the second logging filtered packets:
- `permit host 10.2.3.4`
- `deny log host 10.2.3.5`

The following sets the insertion point before the first rule defined above:
- `before permit host 10.2.3.4`

The following command sets the insertion point after the second rule defined above:
- `after deny log host 10.2.3.5`

The following deletes the first rule defined above:
- `no permit host 10.2.3.4`
deny/permit (by source ICMP packets)

 Filters subscriber sessions based on the internet control message protocol (ICMP) packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-acl)#

Syntax Description
{ deny | permit } { 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 { deny | permit } { 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 { deny | permit } { 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 { deny | permit } { 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.
If the options specified do not exactly match an existing rule, the insertion point does not change.

**Important**

`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.

**Important**

The logging option is not supported for ACLs applied on SPI0 or local contexts.

**source_address**

The IP address(es) from which the packet originated. IP addresses must be entered in IPv4 dotted-decimal format.

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 IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 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.

icmp_type
Specifies that all ICMP packets of a particular type are to be filtered. The type can be an 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 an integer value between 0 and 255.

Usage Guidelines
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. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Examples**
The following commands define two rules with the second logging filtered packets:

```plaintext
permit icmp host 10.2.3.4 any 168
deny log icmp 10.2.3.0 0.0.0.31 host 10.2.4.16 168 11
```

The following sets the insertion point before the first rule defined above:

```plaintext
before permit icmp host 10.2.3.4 any 168
```

The following command sets the insertion point after the second rule defined above:

```plaintext
after deny log icmp 10.2.3.0 0.0.0.31 host 10.2.4.16 168 11
```

The following deletes the first rule defined above:

```plaintext
no permit icmp host 10.2.3.4 any 168
```
deny/permit (by IP packets)

Filters 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

Command Modes: Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

{context_name} host_name(config-acl) #

deny/permit (by IP packets) Command Mode Syntax

deny/permit (by IP packets) Command Mode Syntax Description

deny | permit | log | ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } { fragment | protocol num | after | deny | permit | log | ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } { fragment | protocol num | before | deny | permit | log | ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } { fragment | protocol num | no | deny | permit | log | ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_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.
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 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 IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 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 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 an integer ranging from 0 to 255.
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 Guidelines**

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. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Examples**

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

```
permit ip host 10.2.3.4 any fragment
deny log ip 10.2.3.0 0.0.0.31 host 10.2.4.16
```

The following sets the insertion point before the first rule defined above:

```
before permit ip host 10.2.3.4 any fragment
```

The following command sets the insertion point after the second rule defined above:

```
after deny log ip 10.2.3.0 0.0.0.31 host 10.2.4.16
```

The following deletes the first rule defined above:

```
no permit ip host 10.2.3.4 any fragment
```
deny/permit (by TCP/UDP packets)

Filters 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

Command Modes
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:
{context_name}host_name(config-acl)#

Syntax Description
{ 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 } }

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.

Important
The logging option is not supported for ACLs applied on SPI0 or local contexts.

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) from which the packet originated. IP addresses must be entered in IPv4 dotted-decimal format.
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 IPv4 dotted-decimal notation.

**dest_host_address**  
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

**eq source_port**  
Specifies a single, specific source TCP port number to be filtered.  
source_port must be an integer from 0 through 65535.

**gt source_port**  
Specifies that all source TCP port numbers greater than the one specified are to be filtered.  
source_port must be an integer from 0 through 65535.

**lt source_port**  
Specifies that all source TCP port numbers less than the one specified are to be filtered.  
source_port must be an integer from 0 through 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 an integer from 0 through 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 an integer from 0 through 65535.

**gt dest_port**

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

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

**lt dest_port**

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

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

**range start_port end_port**

Specifies a range of ports to be matched.

`start_port` must be an integer from 0 through 65535, and must be less than the `end_port` value.

`end_port` must be an integer from 0 through 65535, and must be greater than the `start_port` value.
Important

This option is supported in PDIF Release 8.3.

Usage Guidelines

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. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Examples

The following commands define four rules with the second and fourth rules logging filtered packets:

```
permit tcp host 10.2.3.4 any
deny log udp 10.2.3.0 0.0.0.31 host 10.2.4.16
permit tcp host 10.2.3.64 gt 1023 any
deny log udp 10.2.3.0 0.0.0.31 10.2.4.127 0.0.0.127
```

The following sets the insertion point before the first rule defined above:

```
before permit tcp host 10.2.3.4 any
```

The following command sets the insertion point after the second rule defined above:

```
after deny log udp 10.2.3.0 0.0.0.31 host 10.2.4.16
```

The following deletes the third rule defined above:

```
no permit tcp host 10.2.3.64 gt 1023 any
```
description

Allows you to enter descriptive text for this configuration.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**

```
description text
no description
```

- **no**
  Clears the description for this configuration.

- **text**
  Enter descriptive text as an alphanumeric string of 1 to 100 characters.
  If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

**Usage Guidelines**
The description should provide useful information about this configuration.
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

**Usage Guidelines**
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 Description**

exit

**Usage Guidelines**

Use this command to return to the parent configuration mode.
readdress server

Alters 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

Command Modes  Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-acl)#

Syntax Description  

```
readdress server redirect_address | port port_no | { 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 readdress server redirect_address | port port_no | { 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 }

before readdress server redirect_address | port port_no | { 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 }

no readdress server redirect_address | port port_no | { 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 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) 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.
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 IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

eq source_port
Specifies a single, specific source TCP port number to be filtered.
source_port must be an integer from 0 through 65535.

gt source_port
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be an integer from 0 through 65535.

lt source_port
Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be an integer from 0 through 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 an integer from 0 through 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.
**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 an integer from 0 through 65535.

**gt dest_port**

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

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

**lt dest_port**

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

`dest_port` must be an integer 0 through 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 an integer 0 through 65535.

---

**Usage Guidelines**

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. For more information, refer to the Engineering Rules appendix in the System Administration Guide.
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 Release 8.3, for every readdress server rule in an inbound IPv4 ACL, you must add a permit rule to an outbound ACL that explicitly permits packets from the readdress rule's redirect address and port number. If the permit rule is omitted, the system will reject all packets destined for the subscriber's UE from the readdress rule's redirect address and port number.

Examples

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 command 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:

```
no readdress server 192.168.10.4 udp any any
```
redirect context (by IP address masking)

Redirects 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

**Command Modes**

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

{(context_name)host_name(config-acl) #

**Syntax Description**

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

no redirect 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.

**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.
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.

Usage Guidelines
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.
The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important

Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Examples**

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 23 198.162.22.0 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)

Redirects 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

Command Modes
Exec > Global Configuration > Context Configuration > ACL Configuration
configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

/context_name host_name(config-acl)#

Syntax Description
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.
**redirect context (any)**

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

**Important**

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 Guidelines**

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**

Any rule which is added as 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. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important**

Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Examples**

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)

Redirects 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

**Command Modes**

Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-acl)>
```

**Syntax Description**

```
redirect context context_id | log | host source_ipv4_address
after redirect context context_id | log | host source_ipv4_address
before redirect context context_id | log | host source_ipv4_address
no redirect context context_id | log | host source_ipv4_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.
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_ipv4_address**

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

### Usage Guidelines

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. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important**

Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

### Examples

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:

```
beforeredirectcontext23host192.168.200.11
```

The following command sets the insertion point after first the rule defined above:

```
afterredirectcontext23host192.168.200.11
```

The following deletes the first rule defined above:

```
no redirect context 23 host 192.168.200.11
```
redirect context (by source ICMP packets)

Redirects 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

**Command Modes**

Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-acl)#
```

**Syntax Description**

```
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) 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 IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 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.

icmp_type
Specifies that all ICMP packets of a particular type are to be filtered. The type can be an 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 an integer value between 0 and 255.

Usage Guidelines
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.
The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Important Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Examples

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:

```
no redirect context 23 icmp host 192.168.100.25
```
redirect context (by IP packets)

Redirects 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

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-acl)#
```

**Syntax Description**

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]

before 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]

**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 **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 IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 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.

protocol num
Indicates that the packet filtering is to be applied to a specific protocol number.
num can be an integer ranging from 0 to 255.

Usage Guidelines
Block IP packets when the source and destination are of interest.
The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Important

Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Examples

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:

```
noredirect context 23 ip host 198.162.100.25 any fragment
```
redirect context (by TCP/UDP packets)

Redirects 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

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration
conﬁgure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

`(context_name)host_name(config-acl)#`

**Syntax Description**

```bash
redirect context context_id [ 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 redirect context**

```bash
context_id [ 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 ] }
```

**before redirect context**

```bash
context_id [ 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 ] }
```

**no redirect context**

```bash
context_id [ 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 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.

ccontext 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) 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.
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.

**Important**

**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 IPv4 dotted-decimal notation.

**dest_host_address**

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

**eq source_port**

Specifies a single, specific source TCP port number to be filtered.

source_port must be configured to an 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 an integer from 0 through 65535.

**lt source_port**

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be an integer from 0 through 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 an integer from 0 through 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 an integer from 0 through 65535.

**gt dest_port**

Specifies that all destination TCP port numbers greater than the one specified are to be filtered. *dest_port* must be an integer from 0 through 65535.

**lt dest_port**

Specifies that all destination TCP port numbers less than the one specified are to be filtered. *dest_port* must be an integer from 0 through 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 an integer from 0 through 65535.

---

**Usage Guidelines**

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. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

---

**Important**

Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
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 9.0 and later releases, this command is obsoleted.
redirect css service (any)

Redirects subscriber sessions based on any packet received (Content Service Steering). This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration
configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax Description**

```
redirect css service service_name [ log | any
after redirect css service service_name [ log | any
before redirect css service service_name [ log | any
no redirect css service service_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.
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 service_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. service_name must be an alphanumeric string from 1 through 15 characters.

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 Guidelines
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.

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.

The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Examples
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:

```
beforeredirect 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)**

Redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax Description**

```
redirect css service service_name [ log ] host source_host_address
after redirect css service service_name [ log ] host source_host_address
before redirect css service service_name [ log ] host source_host_address
noredirect css service service_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.
redirect css service (by host IP address)

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 service_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. service_name must be an alphanumeric string from 1 through 15 characters.

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 IPv4 dotted-decimal notation.

Usage Guidelines
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
The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Important
Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Examples
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)

Redirects subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

{context_name|host_name}(config-acl)#

**Syntax Description**

redirect css service service_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

before redirect css service service_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

after redirect css service service_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 service_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 |

**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 service_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. service_name must be an alphanumeric string from 1 through 15 characters.

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 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 IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 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.

icmp_type
Specifies that all ICMP packets of a particular type are to be filtered. The type can be an 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 an integer value between 0 and 255.

Usage Guidelines
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

The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Important

Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Examples

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:

```
redirect css service chgsvc1 icmp host 192.168.200.11
```

The following sets the insertion point before the rule definition above:

```
beforeredirect css service chgsvc1 icmp host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 icmp host 192.168.200.11
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 icmp host 192.168.200.11
```
redirect css service (by IP packets)

Redirects subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration

`configure > context context_name > ip access-list acl_name`

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-acl) #
```

**Syntax Description**

```plaintext
redirect css service service_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 service_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 service_name [ log ] ip { any | host source_host_address | source_address source_wildcard 
 } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]

**noredirect css service service_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.
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.

**no**

Removes the rule definition that exactly matches the options specified.

**css service service_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. `service_name` must be an alphanumeric string from 1 through 15 characters.

**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 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 IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 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.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

fragment
Indicates packet redirection is to be applied to IP packet fragments only.

Usage Guidelines
Block IP packets when the source and destination are of interest.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Also note that &quot;redirect&quot; rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.</td>
</tr>
</tbody>
</table>
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 192.168.100.25 any fragment
```

The following sets the insertion point before the rule definition above:

```
beforeredirect css service chgsvc1 ip host 192.168.100.25 any fragment
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 ip host 192.168.100.25 any fragment
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 ip host 192.168.100.25 any fragment
```
redirect css service (by source IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source to the mobile node or the network (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax Description**

```
redirect css service service_name [ log ] source_address source_wildcard
after redirect css service service_name [ log ] source_address source_wildcard
before redirect css service service_name [ log ] source_address source_wildcard
noredirect css service service_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.
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 service_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.

`service_name` must be an alphanumeric string from 1 through 15 characters.

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.

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.

Important

Usage Guidelines

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.
redirect css service (by source IP address masking)

**Important**
The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Examples**
The following command defines a rule definition to redirect packets to a charging service named `chgsvc1`:

```
redirect css service chgsvc1 10.2.3.0 0.0.0.31
```
redirect css service (by TCP/UDP packets)

Redirects subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
{context_name} host_name(config-acl)#
```

**Syntax Description**

```
redirect css service service_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 dest_port | range start_dest_port end_dest_port } }

after redirect css service service_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 dest_port | range start_dest_port end_dest_port } }

before redirect css service service_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 dest_port | range start_dest_port end_dest_port } }

no redirect css service service_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 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.

**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 service_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.
_service_name must be an alphanumeric string from 1 through 15 characters.

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.
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 IPv4 dotted-decimal notation.

**dest_host_address**

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

**eq source_port**

Specifies a single, specific source TCP port number to be filtered. 
*source_port* must be configured to an 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 an 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 an 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 an 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 an 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 `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.

---

**eq destPort**
Specifies a single, specific destination TCP port number to be filtered.

`destPort` must be configured to an integer value from 0 to 65535.

**gt destPort**
Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

`destPort` must be configured to an integer value from 0 to 65535.

**lt destPort**
Specifies that all destination TCP port numbers less than the one specified are to be filtered.

`destPort` must be configured to an integer value from 0 to 65535.

**neq destPort**
Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

`destPort` must be configured to an integer value from 0 to 65535.

**range startDestPort endDestPort**
Specifies that all destination TCP ports within a specific range are to be filtered.

`startDestPort` is the initial port in the range and `endDestPort` is the final port in the range.
Both `startDestPort` and `endDestPort` can be configured to an integer value from 0 to 65535.

---

**Usage Guidelines**
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. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Important

Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Examples

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 command deletes the rule definition above:

```
no redirect css service chgsvc1 udp any
```
redirect css service (for downlink, any)

Redirects subscriber sessions based on any packet received in the downlink (from the Mobile Node) direction (Content Service Steering). This command is also used to set the access control list insertion point.

Product  
All

Privilege  
Security Administrator, Administrator

Command Modes  
Exec > Global Configuration > Context Configuration > ACL Configuration  
configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-acl)#

Syntax Description  
redirect css service service_name [ log ] downlink any 
after redirect css service service_name [ log ] downlink any 
before redirect css service service_name [ log ] downlink any 
no redirect css service service_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 service_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. **service_name** must be an alphanumeric string from 1 through 15 characters.

**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 Guidelines**

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**

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**

The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the **Engineering Rules** appendix in the **System Administration Guide**.

**Important**

Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Examples**

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 downlink any
```
The following sets the insertion point before the rule definition above:
before redirect css service chgsvc1 downlink any

The following command sets the insertion point after the first rule definition above:
after redirect css service chgsvc1 downlink any

The following deletes the first rule definition above:
no redirect css service chgsvc1 downlink any
redirect css service (for downlink, by host IP address)

Redirects subscriber sessions based on the targeted host IP address in the downlink (from the Mobile Node) direction (Content Service Steering).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > ACL Configuration

`configure > context context_name > ip access-list acl_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax Description**

`redirect css service service_name [ log ] downlink host source_host_address`

`before redirect css service service_name [ log ] downlink host source_host_address`

`after redirect css service service_name [ log ] downlink host source_host_address`

`no redirect css service service_name [ log ] downlink 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 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.
redirect css service (for downlink, by host IP address)

**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 service_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. `service_name` must be an alphanumeric string from 1 through 15 characters.

**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 IPv4 dotted-decimal notation.

**Usage Guidelines**
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**
The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Important**
Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Examples**
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 downlink host 192.168.200.11`
The following sets the insertion point before the rule definition above:
**before redirect css service chgsvc1 downlink host 192.168.200.11**

The following command sets the insertion point after the first rule definition above:
**after redirect css service chgsvc1 downlink host 192.168.200.11**

The following deletes the first rule definition above:
**no redirect css service chgsvc1 downlink host 192.168.200.11**
redirect css service (for downlink, by ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets in the downlink (from the Mobile Node) direction (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration
```
configure > context context_name > ip access-list acl_name
```
Entering the above command sequence results in the following prompt:
```
(context_name)host_name(config-acl)>
```

**Syntax Description**
```
redirect css service service_name [ log ] downlink icmp { any | host source_host_address source_wildcard } { any | host dest_host_address dest_wildcard } { icmp_type | icmp_code }
```
```
after redirect css service service_name [ log ] downlink icmp { any | host source_host_address source_wildcard } { any | host dest_host_address dest_wildcard } { icmp_type | icmp_code }
```
```
before redirect css service service_name [ log ] downlink icmp { any | host source_host_address source_wildcard } { any | host dest_host_address dest_wildcard } { icmp_type | icmp_code }
```
```
noredirect css service service_name [ log ] downlink icmp { any | host source_host_address source_wildcard } { any | host dest_host_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 service_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. `service_name` must be an alphanumeric string from 1 through 15 characters.

**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) 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.
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 IPv4 dotted-decimal notation.

**dest_host_address**

The IP address of the destination host to filter against expressed in IPv4 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.

**icmp_type**

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an 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 an integer value between 0 and 255.

**Usage Guidelines**

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*  The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

*Important*  Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Examples**

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 192.168.100.25:

```
redirect css service chgsvc1 downlink icmp host 192.168.100.25
```

The following sets the insertion point before the rule definition above:

```
beforeredirect css service chgsvc1 downlink icmp host 192.168.100.25
```

The following command sets the insertion point after the first rule definition above:

```
afterredirect 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)

Redirects subscriber sessions based on the internet protocol packets in the downlink (from the Mobile Node) direction (Content Service Steering).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-acl)#
```

**Syntax Description**

- `redirect css service service_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 service_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 service_name | log | downlink ip { any | host source_host_address | source_address source wildcard } { any | host dest_host_address | dest_address dest wildcard } [ fragment ]`
- `noredirect css service service_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.

```
css service service_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. `service_name` must be an alphanumeric string from 1 through 15 characters.

```
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) 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 IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 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 Guidelines
Block IP packets when the source and destination are of interest.
The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Examples**

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)

Redirects subscriber sessions based on the IP address mask sent by the source in the downlink (from the Mobile Node) direction (Content Service Steering).

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > ACL Configuration
configure > context context_name > ip access-list acl_name

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

Syntax Description
redirect css service service_name [ log ] downlink source_address source_wildcard
after redirect css service service_name [ log ] downlink source_address source_wildcard
before redirect css service service_name [ log ] downlink source_address source_wildcard
no redirect css service service_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.
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 service_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. `service_name` must be an alphanumeric string from 1 through 15 characters.

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 `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 Guidelines

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

The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Examples

The following command defines a rule definition to redirect packets to a charging service named chgsvc1:

```
redirect css service chgsvc1 downlink 10.2.3.0 0.0.0.31
```
redirect css service (for downlink, by TCP/UDP packets)

Redirects subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the downlink (from the Mobile Node) direction (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration

`configure > context context_name > ip access-list acl_name`

Entering the above command sequence results in the following prompt:

```
{context_name}\host_name(config-acl)#
```

**Syntax Description**

```plaintext
redirect css service service_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 dest_port | range start_dest_port end_dest_port ] }

after redirect css service service_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 dest_port | range start_dest_port end_dest_port ] }

before redirect css service service_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 dest_port | range start_dest_port end_dest_port ] }

no redirect css service service_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 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.

---

**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 service_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. `service_name` must be an alphanumeric string from 1 through 15 characters.

**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 `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 IPv4 dotted-decimal notation.

**dest_host_address**
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

**eq source_port**
Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to an 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 an 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 an 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 an 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 an 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 an 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 an 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 an 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 an 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 an integer value from 0 to 65535.

**Usage Guidelines**

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. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

---

**Important**
Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

---

**Examples**
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:

```plaintext
redirect css service chgsvc1 downlink udp any
```

The following sets the insertion point before the rule definition above:

```plaintext
before redirect css service chgsvc1 downlink udp any
```

The following command sets the insertion point after the first rule definition above:

```plaintext
after redirect css service chgsvc1 downlink udp any
```

The following deletes the rule definition above:

```plaintext
no redirect css service chgsvc1 downlink udp any
```
redirect css service (for uplink, any)

Redirects subscriber sessions based on any packet received in the uplink (to the Mobile Node) direction (Content Service Steering). This command is also used to set the access control list insertion point.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-acl)#

**Syntax Description**

redirect css service service_name [ log ] uplink any
after redirect css service service_name [ log ] uplink any
before redirect css service service_name [ log ] uplink any
no redirect css service service_name [ log ] uplink any

**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**

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.
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 service_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. *service_name* must be an alphanumeric string from 1 through 15 characters.

**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 Guidelines**

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.

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.

The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Examples**

The following command defines a rule definition that redirects packets to the charging service with the name *chgsvc1* and any source IP:

```bash
redirect css service chgsvc1 uplink any
```
The following sets the insertion point before the rule definition above:
`before redirect css service chgsvc1 uplink any`

The following command sets the insertion point after the first 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)

Redirects subscriber sessions based on the targeted host IP address in the uplink (to the Mobile Node) direction (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration
configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax Description**

- **redirect css service service_name [ log ] uplink host source_host_address**
- **after redirect css service service_name [ log ] uplink host source_host_address**
- **before redirect css service service_name [ log ] uplink host source_host_address**
- **noredirect css service service_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.
redirect css service (for uplink, by host IP address)

---

**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 service_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. `service_name` must be an alphanumeric string from 1 through 15 characters.

**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 IPv4 dotted-decimal notation.

---

**Usage Guidelines**

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**
The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

---

**Important**
Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

---

**Examples**

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`:

```bash
redirect css service chgsvc1 uplink host 192.168.200.11
```
The following sets the insertion point before the rule definition above:
before redirect css service chgsvc1 uplink host 192.168.200.11

The following command sets the insertion point after the first rule definition above:
after redirect css service chgsvc1 uplink host 192.168.200.11

The following deletes the first rule definition above:
no redirect css service chgsvc1 uplink host 192.168.200.11
redirect css service (for uplink, by ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets in the uplink (to the Mobile Node) direction (Content Service Steering).

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > ACL Configuration
configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

<context_name>host_name(config-acl) #

Syntax Description
redirect css service service_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 service_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 service_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 service_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

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 service_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. The `service_name` must be an alphanumeric string from 1 through 15 characters.

**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) 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 IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 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.

icmp_type
Specifies that all ICMP packets of a particular type are to be filtered. The type can be an 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 an integer value between 0 and 255.
**Usage Guidelines**

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**

The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

---

**Important**

Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

---

**Examples**

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 command 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 IP packets)

Redirects subscriber sessions based on the internet protocol packets in the uplink (to the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-acl)#

Syntax Description

redirect css service service_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 service_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 service_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 service_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.
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 service_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. `service_name` must be an alphanumeric string from 1 through 15 characters.

**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) 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.

**any**
Specifies that the rule definition applies to all packets.

---

**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.
redirect css service (for uplink, by IP 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 IPv4 dotted-decimal notation.

**dest_host_address**
The IP address of the destination host to filter against expressed in IPv4 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.

**fragment**
Indicates packet redirection is to be applied to IP packet fragments only.

**Usage Guidelines**
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. For more information, refer to the `Engineering Rules` appendix in the `System Administration Guide`.

**Examples**
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:

```bash
after redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

The following command deletes the first rule definition above:

```bash
no redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```
redirect css service (for uplink, by source IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source in the uplink (to the Mobile Node) direction (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-acl)#
```

**Syntax Description**

- `redirect css service service_name [ log | uplink source_address source_wildcard ]`
- `after redirect css service service_name [ log | uplink source_address source_wildcard ]`
- `before redirect css service service_name [ log | uplink source_address source_wildcard ]`
- `no redirect css service service_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 service_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. service_name must be an alphanumeric string from 1 through 15 characters.

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 Guidelines

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

The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Examples

The following command defines a rule definition to redirect packets to a charging service named chgsvc1:

redirect css service chgsvc1 uplink 10.2.3.0 0.0.0.31
redirect css service (for uplink, by TCP/UDP packets)

Redirects subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the uplink (to the Mobile Node) direction (Content Service Steering).

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > ACL Configuration
configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:
{context_name}@host_name(config-acl)#

Syntax Description
redirect css service service_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 dest_port | range start_dest_port end_dest_port } } after redirect css service service_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 dest_port | range start_dest_port end_dest_port } } before redirect css service service_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 dest_port | range start_dest_port end_dest_port } } no redirect css service service_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 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.

css service service_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.
service_name must be an alphanumeric string from 1 through 15 characters.

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 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.
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 IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

eq source_port
 Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to an 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 an 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 an 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 an 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 an 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.
**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 an 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 an 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 an 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 an integer value from 0 to 65535.

**range start_dest_port end_dest_port**

Specifies that all destination TCP port numbers 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 an integer value from 0 to 65535.

---

**Usage Guidelines**

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. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

---

**Examples**

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 (by IP address masking)

Redirects 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

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax Description**

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } | log | source_address source wildcard

after redirect nexthop nexthop_addr { context context_id | interface interface_name } | log | source_address source wildcard

before redirect nexthop nexthop_addr { context context_id | interface interface_name } | log | source_address source wildcard

no redirect 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.
redirect nexthop (by IP address masking)

---

**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 alphanumeric string from 1 to 79 characters.

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.
**Usage Guidelines**

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. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

---

**Important**

Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

---

**Examples**

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)

Redirects 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

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax Description**

```
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
noredirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] any
```

**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.
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.

custom 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 alphanumeric string from 1 to 79 characters.

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 Guidelines
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
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. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Important
Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect nexthop (any)

Examples

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)

Redirects 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

Command Modes: Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

\[context_name\]host_name(config-acl)#

Syntax Description:

- **redirect nexthop** nexthop_addr { context context_id | interface interface_name } [ log ] host
- **after** redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] host
- **before** redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] host

**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.
redirect nexthop (by host IP address)

**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 alphanumeric string from 1 to 79 characters.

```
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_ipv4_address
```
The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

**Usage Guidelines**
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. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important**
Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
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)

Redirects 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

**Command Modes**
Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
/context_name>host_name(config-acl)#
```

**Syntax Description**

```
redirect nexthop
```
```
    nexthop_addr { context context_id | interface interface_name } [ 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 nexthop
```
```
    nexthop_addr { context context_id | interface interface_name } [ 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 nexthop
```
```
    nexthop_addr { context context_id | interface interface_name } [ 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 nexthop
```
```
    nexthop_addr { context context_id | interface interface_name } [ 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.

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 alphanumeric string from 1 through 79 characters.

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.
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 IPv4 dotted-decimal notation.

**dest_host_address**

The IP address of the destination host to filter against expressed in IPv4 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.

**icmp_type**

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an 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 an integer value between 0 and 255.

**Usage Guidelines**

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. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

---

**Important**

Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

---

**Examples**

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)

Redirects 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

Command Modes
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-acl)#

Syntax Description
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 ]

noredirect 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

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 alphanumeric string from 1 through 79 characters.

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.
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.

**Important**

- 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 IPv4 dotted-decimal notation.

- dest_host_address
  The IP address of the destination host to filter against expressed in IPv4 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**

- 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 an integer ranging from 0 to 255.

Usage Guidelines

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. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

---

Important

Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

---

Examples

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 192.168.100.25 any fragment
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25 any fragment
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25 any fragment
```

The following deletes the first rule defined above:

```
noredirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25 any fragment
```
redirect nexthop (by TCP/UDP packets)

Redirects 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

Command Modes
Exec > Global Configuration > Context Configuration > ACL Configuration
configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:
{context_name}@host_name(config-acl)#

Syntax Description
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 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 } before 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.

---

**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 alphanumeric string from 1 through 79 characters.

**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 IPv4 dotted-decimal notation.

**dest_host_address**
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

**eq source_port**
Specifies a single, specific source TCP port number to be filtered.

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

**gt source_port**
Specifies that all source TCP port numbers greater than the one specified are to be filtered.

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

**lt source_port**
Specifies that all source TCP port numbers less than the one specified are to be filtered.

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

`gt dest_port`

Specifies that all destination TCP port numbers greater than the one specified are to be filtered. `dest_port` must be an integer from 0 through 65535.

`lt dest_port`

Specifies that all destination TCP port numbers less than the one specified are to be filtered. `dest_port` must be an integer from 0 through 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 an integer from 0 through 65535.

**Usage Guidelines**

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. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.  

---

Command Line Interface Reference, Commands A - B, StarOS Release 20
Important
Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Examples
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 nexthop 192.168.10.4 context 23 udp any
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 udp any
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 udp any
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 udp any
```
ACS Bandwidth Policy Configuration Mode Commands

The ACS Bandwidth Policy Configuration Mode is used to create and manage Active Charging Service (ACS) Bandwidth Policies.

Note

In 12.3 and earlier releases, a maximum of 64 bandwidth policies can be configured. In 14.0 and later releases, a maximum of 256 bandwidth policies can be configured.

Command Modes

Exec > ACS Configuration > Bandwidth Policy Configuration

**active-charging service** *service_name* > **bandwidth-policy** *policy_name*

Entering the above command sequence results in the following prompt:

[local] *host_name* (config-bandwidth-policy) #

Important

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

- end, page 292
- exit, page 293
- flow limit-for-bandwidth, page 294
- group-id, page 295
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

**Usage Guidelines**
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 Description**
exit

**Usage Guidelines**
Use this command to return to the parent configuration mode.
**flow limit-for-bandwidth**

This command allows you to configure the flow limit-for-bandwidth parameter for the current bandwidth policy.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Bandwidth Policy Configuration

*active-charging service service_name > bandwidth-policy policy_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-bandwidth-policy) #
```

**Syntax Description**

- `flow limit-for-bandwidth id bandwidth_id group-id group_id`
- `no flow limit-for-bandwidth id bandwidth_id`

- **no**
  
  If previously configured, removes the specified flow limit-for-bandwidth configuration in the current bandwidth policy.

- **id bandwidth_id**
  
  Specifies ID for the current bandwidth policy.
  
  `bandwidth_id` must be an integer from 1 through 65535.

- **group-id group_id**
  
  Specifies group ID for the current bandwidth policy.
  
  `group_id` must be an integer from 1 through 65535.

**Usage Guidelines**

Use this command to configure the flow limit-for-bandwidth configuration for a bandwidth policy.

**Examples**

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 allows you to configure the group ID for the current bandwidth policy.

**Product** ACS

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Bandwidth Policy Configuration

```
active-charging service service_name > bandwidth-policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bandwidth-policy)#
```

**Syntax Description**

```
group-id group_id direction { downlink | uplink } peak-data-rate peak_data_rate peak-burst-size peak_burst_size violate-action { discard | lower-ip-precedence } [ committed-data-rate committed_data_rate committed-burst-size committed_burst_size | exceed-action { discard | lower-ip-precedence } ] | { default | no } group-id group_id direction { downlink | uplink }
```

default
Configure this command with default settings for the specified group ID.

no
If previously configured, removes the specified group ID configuration from the current bandwidth policy.

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 peak_data_rate
Specifies the peak data rate, in bits per second.
```
peak_data_rate must be an integer from 1 through 4294967295.
```
Default: 0
peak-burst-size peak_burst_size
Specifies the peak burst size, in bytes.
peak_burst_size 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

committed-data-rate committed_data_rate
Specifies the committed Data Rate, in bits per second. This can also be used to specify the Guaranteed Bit Rate (GBR) for Network Controlled QoS (NCQoS) without exceed-action.
committed_data_rate must be an integer from 1 through 4294967295.
Default: 0

committed-burst-size committed_burst_size
Specifies the committed burst size, in bytes.
committed_burst_size 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 Guidelines
Use this command to configure the Group ID for an bandwidth policy.

Examples
The following command configures the group ID 111 to control bandwidth in 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:

```bash
group-id 111 direction downlink peak-data-rate 10000 peak-burst-size 10000 violate-action discard
```
ACS Charging Action Configuration Mode

The ACS Charging Action Configuration Mode is used to configure Active Charging Service (ACS) charging actions.

Command Modes

Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

Important

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

- allocation-retention-priority, page 299
- billing-action, page 301
- cca charging credit, page 304
- charge-units, page 306
- charge-volume, page 308
- content-filtering processing server-group, page 311
- content-id, page 312
- deactivate-predefined-rule, page 314
- end, page 315
- exit, page 316
- flow action, page 317
- flow idle-timeout, page 324
ACS Charging Action Configuration Mode Commands

- flow limit-for-bandwidth, page 326
- flow limit-for-flow-type, page 329
- ip tos, page 331
- ip vlan, page 333
- nexthop-forwarding-address, page 335
- pco-custom1, page 336
- product-offer-id-avp, page 337
- qos-class-identifier, page 338
- qos-renegotiate, page 339
- retransmissions-counted, page 341
- service-detection, page 342
- service-identifier, page 344
- stripurl token, page 345
- tft packet-filter, page 347
- tft-notify-ue, page 348
- throttle-suppress, page 349
- tos, page 350
- tpo profile, page 352
- video bitrate, page 353
- video cae-readdressing, page 355
- video detailed-statistics, page 357
- video optimization-preprocessing all, page 359
- video optimization-preprocessing cae-readdressing, page 360
- video pacing by-policing, page 361
- xheader-insert, page 363
allocation-retention-priority

This command allows you to configure the Allocation Retention Priority (ARP).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

`active-charging service service_name > charging-action charging_action_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-charging-action)#
```

**Syntax Description**

`allocation-retention-priority priority [pci pci_value | pvi pvi_value]`

`no allocation-retention-priority`

`no`

If previously configured, disables ARP configuration in the current charging action.

`priority`

`priority` must be an integer from 1 through 15.

`pci pci_value`

Specifies the Pre-emption Capability Indicator (PCI).

`pci_value` must be integer 0 or 1.

---

**Important**

If not explicitly enabled, then the default value of 1 will hold true.

`pvi pvi_value`

Specifies the Pre-emption Vulnerability Indicator (PVI).

`pvi_value` must be integer 0 or 1.
If not explicitly enabled, then the default value of 0 will hold true.

**Usage Guidelines**

This command configures the ARP, which indicates the priority of allocation and retention of the service data flow. The ARP resolves conflicts in demand for network resources. At the time of resource crunch, this parameter prioritizes allocation of resources during bearer establishment and modification. In a congestion situation, a lower ARP flow may be dropped to free up capacity. Once a service flow is successfully established, this parameter plays no role in quality of service (QoS) experienced by the flow.

**Examples**

The following command sets the ARP to 10:

```
allocation-retention-priority 10
```
**billing-action**

This command allows you to configure the billing action for packets that match specific rule definitions (ruledefs).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

`active-charging service service_name > charging-action charging_action_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-charging-action)#
```

**Syntax Description**

In StarOS 12.2 and later releases:

```
billing-action { create-edrs { charging-edr charging_edr_format_name | reporting-edr reporting_edr_format_name } + [ wait-until-flow-ends ] | egcdr | exclude-from-udrs | radius | rf } +

no billing-action [ create-edrs | egcdr | exclude-from-udrs | radius | rf ] +
```

In StarOS 12.1 and earlier releases:

```
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 ] +
```

**Important**

This option is available only in 12.1 and earlier releases. In 12.2 and later releases, it is deprecated and is replaced by the `create-edrs charging-edr` option.

Enables EDR billing for packets matching this charging action.

`edr_format_name` must be the name of an existing EDR format, and must be an alphanumeric string of 1 through 63 characters.
If the EDR format name specified 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 create 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.

```
create-edrs { charging-edr charging_edr_format_name | reporting-edr reporting_edr_format_name } +
[ wait-until-flow-ends ]
```

This option is available only in 12.2 and later releases.

Enables EDR billing for packets matching this charging action.

- **charging-edr charging_edr_format_name**: Specifies to generate charging EDR.
  
  charging_edr_format_name must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

- **reporting-edr reporting_edr_format_name**: Specifies to generate reporting EDR.
  
  reporting_edr_format_name must be the name of a reporting EDR format, and must be an alphanumeric string of 1 through 63 characters.

If the above options are 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-CDR billing for packets matching this charging action.

If this option is configured, the system generates an eG-CDR when the subscriber session ends or an interim trigger condition occurs. The interim triggers are configurable in the ACS 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** 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 the Context Configuration Mode.
exclude-from-udrs

By default, statistics are accumulated on a per content ID basis for possible inclusion in UDRs. The `exclude-from-udrs` keyword causes the system not to include the packet's statistics in UDRs.

When this option is disabled, (the default setting) UDRs will be generated based on the UDR format specified in the rulebase.

Default: Disabled.

radius

Enables billing action as RADIUS Charging Data Records (CDRs) for packets matching this charging action, and the data packet statistics will be included in the postpaid RADIUS accounting.

Default: Disabled.

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 ACS Rulebase Configuration Mode.

Usage Guidelines

Use this command to enable an EDR, eG-CDR and/or RADIUS CDR type of billing for content matching this charging action.

Examples

In 12.1 and earlier releases, the following command enables the EDR billing type with EDR format `charge1_format`:

```
billing-action edr charge1_format
```

In 12.2 and later releases, the following command is applied to both charging and reporting EDRs since the trigger for both the EDRs is the same:

```
billing-action create-edrs charging-edr charging_edrformat1 reporting-edr reporting_edrformat1 wait-until-flow-ends
```
**cca charging credit**

This command allows you to enable/disable Credit Control Application (CCA) and configure the RADIUS/Diameter prepaid charging behavior.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-charging-action) #

**Syntax Description**

cca charging credit [ rating-group coupon_id ] [ preemptively-request ]
{ default | no } cca charging

**no**

If previously configured, disables RADIUS/Diameter Prepaid Credit Control Charging in the current charging action.

**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 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.

`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 or not prepaid is enabled.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>This rating-group overrides the content ID, if present in the same charging-action for the prepaid customer in Diameter Credit Control Application (DCCA). But only the content IDs will be used in eG-CDRs irrespective of the presence of rating-group in that charging action.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

**Examples**

The following is an example of this command:

```
cca charging credit
```
charge-units

This command allows you to configure the charge units for RADIUS/DCCA charging calculation.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

Syntax Description

charge-units units

{ default | no } charge-units

default

Configures this command with its default setting.

Default: 0; disables the counter, same as no charge-units

no

If previously configured, disables the charge-units configuration in the current charging action.

units

Specifies 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 Guidelines

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 ACS Ruledef Configuration Mode Commands chapter.
Examples

The following command sets the charging unit to 1024:
charge-units 1024
charge-volume

This command allows you to configure how the volume amount counter for eG-CDRs, UDRs, and DCCA charging are calculated.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Charging Action Configuration

`active-charging service service_name > charging-action charging_action_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

```plaintext
charge-volume {
  { dns | ftp-control | ftp-data | http | icmp | imap | ip | mms | pop3 | pptp | rtcp | rtp | rtsp
  | sdp | secure-http | sip | smtp | tcp | tftp | udp | wsp | wtp }
  { bytes | packet-length | packets }
  { downlink | uplink | constant fixed_value }
  { default | no }
} charge-volume
```

- **default**: Configures this command with its default setting.
  Default: `charge-volume ip bytes`

- **no**
  If previously configured, deletes the charge-volume configuration in the current charging action.

```plaintext
{ dns | ftp-control | ftp-data | http | icmp | imap | ip | mms | pop3 | pptp | rtcp | rtp | rtsp
  | sdp | secure-http | sip | smtp | tcp | tftp | udp | wsp | wtp }
```

Specifies the charge volume method for the specific rule definition.

- **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
• **pptp**: Charge volume for PPTP
• **rtcp**: Charge volume for RTCP
• **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
• **tftp**: Charge volume for TFTP
• **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** `fixed_value`
This sets the fixed increment value for charging.
`fixed_value` 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 Guidelines**
This command provides the method for charging volume calculation for different protocols and packets.
For information on supported protocols see the *ACS Ruledef Configuration Mode Commands* chapter.
If **charge-volume rtp packets** is configured, system computes volume amounts for different options for RTP as follows:
### 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).

### Examples

Following command sets the charging volume of downlink packets for RTP:

```bash
charge-volume rtp packets downlink
```
content-filtering processing server-group

This command allows you to enable/disable Category-based Content Filtering.

**Product**

CF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

```
content-filtering processing server-group
{ default | no } content-filtering processing
```

- **default**
  - Configures this command with its default setting.
  - Default: Content filtering configured for the rulebase is attempted

- **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 Guidelines**

Use this command to enable or disable Category-based Content Filtering in the charging action.

This command works as second-level filter to process the HTTP/WAP GET request with Internet Content Adaptation Protocol (ICAP) after ruledef matching. The first-level filtering is in the rulebase configuration. This CLI command is only effective when the **content-filtering mode server-group** command is configured in the rulebase.

**Examples**

The following command enables content filtering in the current charging action:

```
content-filtering processing server-group
```
**content-id**

This command allows you to specify the 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 the Diameter Credit Control Application (DCCA).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-charging-action)#
```

**Syntax Description**

- `content-id content_id`
- `no content-id`

`content_id`

Removes the content ID configuration from the charging action.

**Usage Guidelines**

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 *ACS Ruledef Configuration Mode Commands* chapter.
Examples

The following command sets the content ID in the current charging action to 23:

```
content-id 23
```
deactivate-predefined-rule

This command allows you to remove or deactivate the matched predefined rule/Group of Ruledefs (activated by PCRF via Gx) that selected this action to ensure one time redirection for the subscriber.

Product
GGSN, P-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Charging Action Configuration
active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-charging-action) #

Syntax Description
| default | no | deactivate-predefined-rule |

default
Configures this command with its default setting.
Default: Disabled; same as no deactivate-predefined-rule

no
If previously enabled, disables the predefined rule in the current charging action.

Usage Guidelines
Use this command to ensure that the predefined rule/Group of Ruledefs gets deactivated after applying the charging-action when configured. By default, the configuration is disabled. Static rules are not deactivated by this command.

This feature is added in the ECSv2 to redirect traffic when quota for a user expires. When quota expires, PCRF will install a rule for the redirection. In the charging-action for this redirection rule, an action to disable the same rule will ensure one time redirection. A charging-rule-report will be sent to PCRF indicating the PCC Rule Status as INACTIVE for the deactivated rule. Rule-Failure-Code sent is RESOURCE_ALLOCATION_FAILURE.

The deactivation will apply only for predefined rules/Group of Ruledefs. If a static rule is associated with the charging-action, it will not be deactivated.
end

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

**Product**: All

**Privilege**: Security Administrator, Administrator

**Syntax Description**: end

**Usage Guidelines**: 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 Description
exit

Usage Guidelines
Use this command to return to the parent configuration mode.
flow action

This command allows you to specify the action to take on packets that match rule definitions.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-charging-action)#
```

**Syntax Description**
In StarOS 12.2 and later releases:

```
flow action { conditional user-agent end-token end_token_name | discard | downlink | uplink | random-drop interval_start to interval_end pkts-to-drop packet_min to packet_max | readdress [ [ server ipv4_address/ipv6_address | discard-on-failure | [ dns-proxy-bypass ] | [ port port_number | discard-on-failure | [ dns-proxy-bypass ] | [ server-list server_list_name | hierarchy ] | round-robin ] | dns-proxy-bypass ] | discard-on-failure ] | [ redirect-ocs-url | redirect-url redirect_url ] | [ encryption { blowfish128 | blowfish64 } | { aes128 | aes256 } [salt] } ] | encrypted | key key | clear-quota-retry-timer | [ first-request-only | post-redirect { allow | discard | terminate } ] ] ] | rulebase-change rulebase_name | terminate-flow | terminate-session | url-readdress server ipv4_address | port port_number ]
```

```
no flow action
```

In StarOS 12.1 and earlier releases:

```
flow action { conditional user-agent end-token end_token_name | discard | downlink | uplink | random-drop interval_start to interval_end pkts-to-drop packet_min to packet_max | redirect-url redirect_url | clear-quota-retry-timer | [ readdress [ server ipv4_address/ipv6_address ] | [ port port_number ] ] | terminate-flow | terminate-session }
```

```
no
```

If previously configured, deletes the flow action configuration in the current charging action.

**conditional user-agent end-token end_token_name**

Specifies to conditionally redirect 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 ACS Configuration Mode. *end_token_name* must be an alphanumeric string of 1 through 32 characters, and is configured with this command to end the redirection condition.
**discard | downlink | uplink**

Specifies to discard the specified packets.

- **downlink**: Downlink packets
- **uplink**: Uplink packets

If **downlink** or **uplink** keyword is not specified, both downlink and uplink packets will be discarded.

**random-drop interval interval_start to interval_end pkts-to-drop packet_min to packet_max**

Specifies to drop a group of consecutive packets (pkts-to-drop) to be dropped in the specified time interval (random-drop interval). This will cause degradation in user experience. P2P VoIP would need more than one packet to be dropped, since that type of protocol is geared to handle occasional single packet drops.

- **random-drop interval 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 ipv4_address/ipv6_address | discard-on-failure | [ dns-proxy-bypass ] | [ port port_number | discard-on-failure | [ dns-proxy-bypass ] | [ server-list server_list_name | hierarchy | round-robin | [ discard-on-failure | [ dns-proxy-bypass ] | ]

Specifies to readdress the location of the uplink packets for charging action.

- **server ipv4_address/ipv6**: Specifies the re-address server's IPv4/IPv6 address.
- **port port_number**: Specifies the re-address server's port number.
  - *port_number* must be an integer from 1 through 65535.

  **Important** You can optionally keep the original destination address and just change the destination TCP/UDP port number.

- **server-list server_list_name**

  **Important** This option is available only in StarOS 14.1 and later releases.
  - This keyword is license dependent. For more information please contact your Cisco account representative.

  Specifies to readdress the packet flow to the DNS servers configured under the server list.
  For more information about configuring the server list, see the ACS Readdress Server List Configuration Mode chapter.

- **hierarchy**
  - Specifies the hierarchy approach to select the server list from the readdress server list.
• **round-robin**

  Specifies the round-robin approach to select the server list from the readdress server list. This is the default approach.

• **discard-on-failure**

  
  This option is available only in StarOS 14.0 and later releases.

  Specifies to discard the packets if readdressing fails due to duplicate key. If this keyword is not configured, no action is taken and the packets are allowed to pass.

  If already configured, to revert the behavior, configure the `flow action readdress` command again without the `discard-on-failure` keyword.

• **dns-proxy-bypass**

  
  This option is available only in StarOS 12.3 and later releases.

  Specifies the DNS packets to bypass interception at the session manager when readdressing for flow occurs, and go through ECS-based DNS redirection. If this keyword is not configured, DNS redirection from ECS is disabled.

**redirect-ocs-url**

  This option is available only in StarOS 12.3 and later releases.

  Specifies to redirect to the URL provided by OCS only for post-processing dynamic rules.

  
  `redirect-url redirect_url [ [ encryption { blowfish128 | blowfish64 } | { { aes128 | aes256 } [salt] } ] ] [ encrypted ] key key [ [ clear-quota-retry-timer ] [ first-request-only ] [ post-redirect { allow | discard | terminate } ] ] ]`

  Specifies to return a redirect response to the subscriber, and terminate the TCP connections (to the subscriber and server). The subscriber's Web browser should automatically send the original HTTP packet to the specified URL. Redirection is only possible for certain types of HTTP packets (for example, GET requests), which typically are only sent in the uplink direction. If the flow is not HTTP, the `redirect-url` option is ignored, that is the packet is forwarded normally, except for SIP. For SIP, a Contact header with the redirect information is inserted.

  The redirect-url consists of the redirect url and may additionally include one or more dynamic fields. Earlier, the dynamic fields could be encrypted using 128 and 256 bit blowfish encryption. The new functionality provides the additional AES-CBC encryption of the dynamic fields as well.

  • **redirect_url** specifies the redirect URL. `redirect_url` must be an alphanumeric string of 1 through 511 characters. It may include one or more dynamic fields (up to 16 may be specified). For example, `http://search.com/subtarg=#HTTP.URL#`

  Dynamic fields must be enclosed in "#" (hash).

  Up to 16 dynamic fields out of the following 23 are allowed:
Concatenated fields separated by ; (semi colon) can also be inserted. For example, #BEARER.IMSI;BEARER.IMEI#

- **encryption** { blowfish128 | blowfish64 } [ ] { { aes128 | aes256 } [salt] } }encrypted | key key

---

**Important**

This option is available only in StarOS 12.2 and later releases.

**encryption**: Specifies to enable encryption for dynamic fields of the redirect URL.

- **blowfish128**: Specifies to use Blowfish encryption with 128 bit key for encrypting the dynamic fields.
- **blowfish64**: Specifies to use Blowfish encryption with 64 bit key for encrypting the dynamic fields.
- **aes128**: Specifies to use AES-CBC encryption with 128 bit key for encrypting the dynamic fields.
- **aes256**: Specifies to use AES-CBC encryption with 256 bit key for encrypting the dynamic fields.
- **salt**: Specifies to use salt with AES-CBC encryptions of the dynamic fields.
- **encrypted**: Specifies to encrypt the key.
- **key key**: Specifies the key to use for encryption of dynamic fields.
  
  *key* must be an alphanumeric string of 1 through 523 characters.

Note that encryption is supported only for the following fields:

- **#BEARER.CALLING-STATION-ID#**
- **#BEARER.MSISDN#**
- **#BEARER.IMEI#**
- **#BEARER.MEID#**
- **#BEARER.IMSI#**
- **#BEARER.USERNAME#**
- **#BEARER.ESN#**

Also, concatenated fields having any of the above will be encrypted.

%3furl= can be used as a delimiter between URL. As in `http://search.com/subtarg/%3furl=#HTTP.URL#` format.

- **clear-quota-retry-timer**: Specifies to reset Credit Control Application (CCA) Quota Retry Timer upon redirection.
- **first-request-only | post-redirect { allow | discard | terminate } |**

  **Important** This option is available only in StarOS 12.3 and later releases.

- **first-request-only**: Specifies the url-redirection to be performed only once per session after the first web traffic has been detected.
- **post-redirect**: Specifies the action to be taken on subsequent flow packets that invoke this charging action after the first url-redirection has been performed for that session.

The following are the different actions allowed on the flow packets:

- **allow**: allows the packets subsequent to the first url-redirection to flow
- **discard**: discards the packets subsequent to the first url-redirection
- **terminate**: terminates the flow of packets on receiving packets subsequent to the first url-redirection
To disable this option if configured earlier, reuse the same `flow action redirect-url` command without the `first-request-only` keyword.

---

**Important** Disabling the `first-request-only` keyword will not affect the existing subscriber calls.

---

**rulebase-change `rulebase_name`**

Specifies the rulebase to change to when the charging action is applied. The new rulebase will be applied to the next packet on the call, and applied only to the current PDN.

**terminate-flow**

Specifies to terminate the 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 applicable only for flows that use TCP.

**terminate-session**

Specifies to terminate the session.

When a rule pointing to a charging action configured with the terminate-session keyword is hit, then the corresponding session will be terminated.

**url-readdress server `ipv4_address` [ `port port_number` ]**

Configures the URL server to re-address for the specified charging action.

- **server `ipv4_address`**: Specifies the re-address server's IPv4 address.
- **port `port_number`**: Specifies the re-address server's port number.

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

**Usage Guidelines**

Use this command to specify the action to take on packets, for example to discard, terminate, or redirect.

When a readdress server is configured for a charging action, the `show configuration` command will display the readdress related configuration only if server address is configured. The `show configuration verbose` command will display the readdress sever if configured, else will display "no flow action".

The redirect-url option 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
```
This would mean any SIP request that hits the sip_req rule def, 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".

Examples

The following command sets the flow action to terminate:

```
flow-action terminate-flow
```

The following command resets quota retry timer upon redirection of flow to HTTP URL http://search.com/?url=#http://msn.com#:

```
flow action redirect-url http://search.com/%3url=#http://msn.com# clear-quota-retry-timer
```
flow idle-timeout

This command allows you to configure the maximum duration a flow can remain idle after which the system automatically terminates the flow.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

Syntax Description

flow idle-timeout { idle_timeout | flow-mapping flow_timeout }
{ default | no } flow idle-timeout [ flow-mapping ]

no

Disables the idle-timeout configuration; sets the idle-timeout to 0 seconds.

default

Configures this command with its 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.

flow-mapping flow_timeout

Specifies the maximum duration of flow-mapping timeout, in seconds.

flow_timeout must be an integer from 0 through 86400.

Usage Guidelines

Use this command to configure the maximum duration a flow can remain idle after which the system automatically terminates the flow.
Examples

The following command configures the idle-timeout setting to 400 seconds:

flow idle-timeout 400
Flow Limit-For-Bandwidth

For Session Control functionality this command allows you to enable/disable bandwidth limiting and configure the uplink and downlink bandwidth limits for subscriber.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

**Syntax Description**

```
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**

If previously configured, disables bandwidth control traffic policing for the specified direction for the current subscriber.

**default**

Configures this command with its default setting.

**direction { downlink | uplink }**

Specifies the direction of flow to apply bandwidth limit:

- **downlink**: Flow of data towards subscriber.
- **uplink**: Flow of data from subscriber.

**peak-data-rate bps**

Specifies the peak data-rate for the subscriber, in bps (bits per second).

*bps* must be an integer from 1 through 4294967295.

Default: 256000
**peak burst-size bytes**
The peak burst size allowed, in bytes.
*bytes* must be an integer from 1 through 4294967295.
Default: 3000

---

**Important**
It is recommended that this parameter be configured to at least the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

---

**violate-action { discard | lower-ip-precedence }**
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

Default: **discard**

**committed-data-rate bps**
The committed data rate (guaranteed-data-rate) in bits per second (bps).
In releases prior to 15.0, the committed-data-rate based policing was not effected for non-GBR bearers even if it is configured in Charging Action configuration mode. In 15.0 and later releases, the committed-data-rate policing can be implemented for both GBR bearers and non-GBR bearers. If the customer does not want to implement the committed-data-rate policing for non-GBR bearers, then the **committed-data-rate** keyword should not configured with the **flow limit-for-bandwidth** command in Charging Action configuration mode.
*bps* must be an integer from 1 through 4294967295.
Default: 144000

**committed-burst-size bytes**
The committed burst size allowed, in bytes.
*bytes* must be an integer from 1 through 4294967295.
Default: 3000

**exceed-action { discard | 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.
Default: **lower-ip-precedence**
id id

**Important**

This option is available only in StarOS 8.1 and later releases.

Specifies the bandwidth limiting identifier.

*id* 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 the content ID.

**Usage Guidelines**

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.

More information on the QoS feature is available in the *QoS Management appendix* of the *System Administration Guide*.

**Examples**

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 allows you to specify the maximum number of simultaneous flows (of this type) that a subscriber may have, and the action to take if the limit is reached.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

`active-charging service service_name > charging-action charging_action_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

`flow limit-for-flow-type limit over-limit-action { discard | redirect-url url | terminate-flow | terminate-session }`

`no flow limit-for-flow-type`

`no`

If previously configured, deletes the flow limit-for-flow-type configuration in the current charging action.

`limit`

Specifies the maximum number of flows of a type exceeding which the specified over-limit-action triggers. `limit` must be an integer from 1 through 4000000000.

`over-limit-action { discard | redirect-url url | terminate-flow | terminate-session }`

Specifies the action to take on exceeding `limit` for a flow type:

- **discard**: Discards the packets
- **redirect-url url**: Redirects the flow to the specified URL. `url` must be an alphanumeric string of 1 through 511 characters. For example, http://search.com.
- **terminate-flow**: Terminates the flow to which this packet belongs
- **terminate-session**: Terminates the session to which this packet belongs
**Usage Guidelines**

Use this command to specify the number of simultaneous flows (of a type) that a subscriber may have, and the action to take if the limit is reached.

All flows with the same content-id are considered to be the same type. This limit applies to the total of all flows for a subscriber connection (that is, an individual PDP context or individual A10 tunnel).

If the flow is not HTTP, the redirect-url option is ignored, that is the packet is forwarded normally. Refer to the **flow action** CLI command.

If the limit specified by the **flow limit-across-applications** command in the Rulebase Configuration Mode is also exceeded, action is taken for that over-limit condition rather than the action configured here.

**Examples**

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 allows you to configure the IP Type of Service (ToS) octets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Charging Action Configuration  
active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

**Syntax Description**

```bash
ip tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | lower-bits
tos_value } [ uplink | downlink ]
{ default | no } ip tos | uplink | downlink }

default
Configures this command with its default setting.
Default: IP ToS is not modified.

no
If previously configured, deletes the IP ToS configuration in the current charging action.

af.xx
Specifies the use of an assured forwarding xx per hop behavior (PHB).

be
Specifies the use of best effort forwarding PHB.

ef
Specifies the use of expedited forwarding PHB.
lower-bits tos_value

In StarOS 8.1 and later releases, this option is "lower-bits tos_value". In StarOS 8.0, it is tos_value.

Specifies 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 only for downlink packets.

uplink

Specifies the ToS only for uplink packets.

Usage Guidelines

Use this command to specify the IP Type of Service (ToS) octets to use 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.

If downlink or uplink keywords are not specified, the command applies to both directions.

This command may be used multiple times. For example, the following sequence of commands will cause to set the ToS to af11 in the uplink direction, but not modify the ToS in the downlink direction:

```
ip tos af11
no ip tos downlink
```

Examples

The following command sets the IP ToS to be with downlink:

```
ip tos be downlink
```
ip vlan

This command allows you to configure the VLAN identifier to be associated with the subscriber traffic in the destination context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

```
ip vlan vlan_id
{ default | no } ip vlan
```

**default**

Configures this command with its default setting.

Default: Disable this IP VLAN configuration. Same as `no ip vlan` command.

**no**

If previously configured, deletes the IP VLAN configuration in the current charging action. Whatever value is configured for the VLAN tag in the subscriber configuration or IP pool configuration (or no VLAN tag if there is no configuration elsewhere) is used.

```
vlan_id
```

Specifies the VLAN ID.

`vlan_id` must be an integer from 1 through 4094.

**Usage Guidelines**

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.

**Examples**

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 allows you to configure the nexthop forwarding address.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

`active-charging service service_name > charging-action charging_action_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-charging-action)#
```

**Syntax Description**

`nexthop-forwarding-address ipv4_address`

`no nexthop-forwarding-address`

`no`

If previously configured, deletes the nexthop-forwarding-address configuration in the current charging action.

`ipv4_address`

Specifies the nexthop-forwarding-address for the current charging action.

`ipv4_address` must be the nexthop forwarding address, and must be an IPv4 address.

**Usage Guidelines**

Use this command to configure the nexthop-forwarding-address for a charging action. When an uplink packet matches a rule and a charging action is applied to it this nexthop forwarding address is used.

There are different methods to configure a nexthop forwarding address, they are prioritized as follows:

- The nexthop forwarding address, if configured, in a redirect ACL is used
- Else, the nexthop address configured in the charging action is used
- Else, the nexthop address, if configured, in the IP pool is used

**Examples**

The following command sets the nexthop forwarding address for the current charging action to 10.1.1.1:

`nexthop-forwarding-address 10.1.1.1`
**pco-custom1**

This command configures the Protocol Configuration Options (PCO) value that will be sent to all UEs, and relates to the PCO for UE Notification feature.

**Product**
P-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Charging Action Configuration

`active-charging service service_name > charging-action charging_action_name`

Entering the above command sequence results in the following prompt:

`[local] host_name(config-charging-action)#`

**Syntax Description**

`pco-custom1 custom1_value`

`{ no | default } pco-custom1`

**default**
Configures custom1 with the default setting.
Default: 0

**no**
If previously configured, resets the pco-custom1 value to the default setting.

**custom1_value**
Specifies the PCO custom1 value.

*custom1_value* must be an integer from 0 through 255.

**Usage Guidelines**

Use this command to configure the PCO custom1 value to be sent to the MS GTP messages. To enable or disable sending customized PCO options, use the **pco-options** command in the APN Configuration Mode.

**Examples**
The following command configures PCO custom1 value to 5:

`pco-custom1 5`
product-offer-id-avp

This command enables sending the "Product-Offer-ID" AVP with traffic identifier for Home Agent (HA)/Content Charging Gateway (CCG) instead of the "Rating-Group" AVP. This allows to identify and report application service traffic interval or volume.

Important This command is customer-specific. For more information please contact your Cisco account representative.

Product

HA
PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-charging-action)#

Syntax Description

product-offer-id-avp

Usage Guidelines

Use this command to send the "Product-Offer-ID" AVP in Diameter message instead of the "Rating-Group" AVP for HA/CCG implementation. This implementation means that HA/CCG is deployed to work with both AAA server and OCS via Diameter Gy Online Charging Protocol for content based billing on both offline and online charging.

Important If there is no mapping label configured for a content-id with the label content-id command in Active Charging Service Configuration Mode, the rating group will be sent in Product-Offe-ID AVP as Label.
qos-class-identifier

This command allows you to configure the QoS Class Identifier (QCI).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

Syntax Description

qos-class-identifier qos_class_identifier

no qos-class-identifier

no

If previously configured, deletes the QCI configuration in the current charging action.

qos_class_identifier

Specifies the QCI.

qos_class_identifier must be an integer from 1 through 9 or from 128 through 254 (Operator specific).

Usage Guidelines

Use this command to configure the QCI for a charging action.

 Examples

The following command configures the QCI as 3:

qos-class-identifier 3
qos-renegotiate

This command allows you to configure the QoS traffic class for the Layer 7 QoS Renegotiation feature, enabling the triggering of QoS renegotiation from a rule.

Important
This command is license dependent. For more information please contact your Cisco account representative.

Product
GGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

Syntax Description

qos-renegotiate traffic-class { background | conversational | interactive priority | streaming }

no qos-renegotiate

no
If previously configured, deletes the qos-renegotiate traffic-class configuration in the current charging action.

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 Guidelines
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.

Examples
The following command sets the QoS traffic class in the charging action to streaming:

```
qos-renegotiate traffic-class streaming
```
retransmissions-counted

This command allows you to specify whether to count (for billing purposes) the number of packet retransmissions.

**Important**
In release 17.0, this command has been deprecated. This configuration is available at rulebase level as [local] host_name(config-rule-base)# [no] retransmissions-counted.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Charging Action Configuration

**Syntax Description**
[ default | no ] retransmissions-counted

default
Configures this command with its default setting.
Default: Disabled; same as no retransmissions-counted

no
If previously enabled, disables the retransmissions-counted configuration in the current charging action.

**Usage Guidelines**
Use this command to enable counting of the number of retransmissions.

If not enabled, retransmissions are automatically detected but discounted. The retransmissions will still be analyzed by the TCP analyzer (and higher layer analyzers), but the statistics (except for the count of retransmissions) will not be updated. Also, some higher layer analyzers (MMS, SIP, WSP, and WTP) can detect retransmissions when UDP is the transport layer.

**Examples**
The following is an example of this command:
retransmissions-counted
**service-detection**

The **service-detection session-update** command enables the support for users' QoS updation by PDSN/PCEF based on service start or stop.

---

**Important**
This command is customer specific. For more information contact your Cisco account representative.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Command Modes**

- Exec > ACS Configuration > Charging Action Configuration
- active-charging service *service_name* > charging-action *charging_action_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-charging-action)#
```

**Syntax Description**

- service-detection session-update qos
- no service-detection session-update

**Usage Guidelines**

Use this command to configure the service detection to enable the support for users' QoS updation by PDSN/PCEF based on service start or stop.

- no
  If previously configured, deletes the service-detection configuration in the current charging action.

- service-detection
  Detects start or end of service on PDSN

- session-update
  Updates the subscriber session

- qos
  Sets qos updation (upgrade/downgrade)
Examples

The following command configures service detection for a subscriber session and sets the QoS updation.

```
service-detection session-update qos
```
service-identifier

This command allows you to configure the service identifier to use in the generated billing records, as well as the AVP used by the Credit Control Application, such as the "Service-Identifier" AVP for use by DCCA. This is a more general classifier than content-id.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-charging-action) #
```

**Syntax Description**

```
service-identifier service_id
no service-identifier
```

**no**
If previously configured, deletes the service ID configuration in the current charging action.

```
service_id
```

Specifies the service identifier.

In 12.1 and earlier releases `service_id` must be an integer from 1 through 65535.

In 12.2 and later releases, `service_id` must be an integer from 1 through 2147483647.

**Usage Guidelines**
Use this command to configure the service identifier to use in generated billing records, as well as the AVP used by the Credit Control Application, such as the "Service-Identifier" AVP for use by DCCA. This is a more general classifier than content-id.

**Examples**
The following command configures the service identifier in the current charging action to 99:

```
service-identifier 99
```
stripurl token

This command allows you to configure the token and value to be stripped from the HTTP URL.

Important

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product

MVG

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Charging Action Configuration
active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

Syntax Description

stripurl token token_name [ value token_value ]
no stripurl

no

If previously configured, disables the URL stripping configuration in the current charging action

token token_name

Specifies the name of the token to be stripped from the URL. The stripurl token command is case-sensitive. Hence if the token name does not match, then charging action will not be applied.

token_name must be an alphanumeric string of 1 through 127 characters.

value token_value

Specifies the value of the token to be stripped from the URL.

token_value must be an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to configure the token and value to be stripped from the HTTP URL.
Examples

For the given URL: http://www.videoserver.com?Name1=val1&Name2=val2&Name3=val3, if the following CLI is used, this will strip parameter Name2 and its optional value val2 from the above URL and gives the following new URL: http://www.videoserver.com?Name1=val1&Name3=val3:

stripurl token Name2 value val2
tft packet-filter

This command allows you to specify the packet filter to use in TFTs sent to the MS.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

Syntax Description

| no | tft packet-filter packet_filter_name

no
If previously configured, removes the specified packet filter from the current charging action.

packet_filter_name
Specifies the packet filter to add/remove from the current charging action.
packet_filter_name must be the name of a packet filter, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

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.

Examples

The following command configures the packet filter filter23 to be sent to the MS:

tft packet-filter filter23
**tft-notify-ue**

This command allows you to control whether TFT updates are sent to UE or not.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

`active-charging service service_name > charging-action charging_action_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

| no | tft-notify-ue |

**Usage Guidelines**

Use this command to suppress the selected TFT updates from being sent to the UE. This helps to identify if the appropriate TFT defined in the charging action needs to be sent to the UE or not. This CLI command is supported for both default and dedicated bearers.

The ability to include TFTs in the initial session creation are also controlled through this command. This way, the operator can suppress any unwanted TFTs to the UE.

Releases prior to 15.0, all predefined rules charging actions are associated with TFTs and the system includes TFTs towards the UE for all scenarios. In some scenarios it results in creating duplicate TFTs. This CLI-based approach is developed to overcome this situation.

NOTE: The TFT updates are not sent to UE based on certain trigger conditions.
**throttle-suppress**

This command allows you to suppress bandwidth limiting at charging-action, bearer, and APN level.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

```plaintext
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

```
throttle-suppress [ timeout suppress_timeout ]
no throttle-suppress
```

- **timeout suppress_timeout**

  Specifies the time for which bandwidth limiting is suppressed, in seconds.
  
  `suppress_timeout` must be an integer from 10 through 300.

  Default: 30 seconds

- **no**

  If configured, bandwidth limiting will continue from the next flow onwards.

- **Usage Guidelines**

  Use this command to suppress bandwidth limiting (throttling) at charging-action, bearer, and APN level. When `throttle-suppress` is configured, the timeout will take the default value of 30 seconds and the flow will not be throttled for the next 30 seconds. When configured with the `timeout` keyword, bandwidth limiting is suppressed for the mentioned time.

- **Examples**

  The following command suppresses the flow (PDP context) for the next 155 seconds when traffic hits the charging-action:

  ```plaintext
  throttle-suppress timeout 155
  ```
tos

This command allows you to configure the Type of Service (ToS) octets.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-charging-action) #

Syntax Description
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.

af xx

Specifies the use of an assured forwarding xx Per Hop Behavior (PHB).

be

Specifies use of Best Effort forwarding PHB.

ef

Specifies use of Expedited Forwarding PHB.

lower-bits tos_value

Important
In StarOS 8.1 and later releases, this option is "lower-bits tos_value". In StarOS 8.0 release, 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 only for downlink packets.

uplink
Specifies the ToS only for uplink packets.

Usage Guidelines
Use this command to set the ToS octets used in the charging action. If one of the enumerated values is set, the Differentiated Services Code Point (DSCP) bits (the six most-significant bits (MSBs) in the ToS byte) are marked. If the integer value is set, it will be written into the six least-significant bits (LSBs) of the ToS byte.

Examples
The following command sets the ToS to \textit{be} for downlink packets:
\texttt{tos be downlink}
tpo profile

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
video bitrate

This command allows you to specify the default target bit rate to use for the video pacing feature on the Mobile Video Gateway. This value is also used as the suggested maximum bit rate for the video optimization policy control feature.

Important

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product

MVG

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Syntax Description

[ default | no | video bitrate bit_rate [ -noconfirm ] ]

default

Sets video bitrate to its default value.

no

Deletes the video bit rate if previously configured.

video bitrate bit_rate

Specifies the bit rate, in bits per second, at which the TCP video flow should be paced during video pacing. This value is also used as the suggested maximum bit rate for the video optimization policy control feature. For video pacing, this default bit rate is used on each video flow until the rate determination function calculates the optimal bit rate for pacing.

bit_rate must be an integer from 0 to 256000000.

Default: 0
-noconfirm
Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**
Use this command to specify the default bit rate to use for the video pacing feature, and the suggested maximum bit rate for the video optimization policy control feature.

**Examples**
The following command sets the bit rate for the video flow at 300000 (300kbps):
`video bitrate 300000`
video cae-readdressing

This command allows you to enable CAE (Content Adaptation Engine) re-addressing, allowing video traffic to be fetched from the CAEs in the CAE group. The CAE is an optional component of the Mobile Videoscape.

**Important**
In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product**
MVG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Charging Action Configuration

```
active-chargingservice service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-charging-action)#
```

**Syntax Description**
```
[ no ] video cae-readdressing [ xheader-format xheader_format_name ]
```

**no**
Disables CAE re-addressing if previously configured.

**video cae-readdressing**
Enables CAE re-addressing, allowing video traffic to be fetched from the CAEs in the CAE group.

**xheader-format xheader_format_name**
Specifies an HTTP x-header (Extension header) format for readdressing. When specified, the MVG inserts a destination IP address and TCP port number in a proprietary HTTP x-header in the HTTP request to the CAE. The CAE uses this information to connect to the OS (Origin Server) to retrieve selected video clips for adaptation.

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

**Usage Guidelines**
Use this command to enable CAE re-addressing on the Mobile Video Gateway.
Examples

The following command enables CAE re-addressing:

```
video cae-readdressing xheader-format format_1
```
video detailed-statistics

This command allows you to enable the collection of detailed video statistics.

Important

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product

MVG

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-charging-action)#

Syntax Description

| default | no | video detailed-statistics | -noconfirm |

default

Sets video detailed-statistics to its default value, which is the same as [ no ].

no

Disables the video statistics feature if previously enabled.

video detailed-statistics

Enables the video statistics feature. When a flow matches a rule definition for video during DPI (Deep Packet Inspection), the video statistics feature begins collecting detailed statistics for the video flow.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to enable the video statistics feature.
The following command enables the video statistics feature:

```
video detailed-statistics
```
**video optimization-preprocessing all**

This command allows you to enable CAE re-addressing by enabling the Active Charging Service (ACS) to re-address video requests to the CAEs in the CAE group.

---

**Important**

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

---

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

`active-charging service service_name > charging-action charging_action_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

| no | video optimization-preprocessing all |

no

Disables CAE re-addressing if currently enabled.

**Usage Guidelines**

Use this command to enable CAE re-addressing by enabling the ACS to re-address video requests to the CAEs in the CAE group.

**Examples**

The following command enables CAE re-addressing:

`video optimization-preprocessing all`
video optimization-preprocessing cae-readdressing

This command allows you to enable CAE re-addressing by enabling the Active Charging Service (ACS) to re-address video requests to the CAEs in the CAE group.

**Important**

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

`active-charging service service_name > charging-action charging_action_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-charging-action) #
```

**Syntax Description**

| no | video optimization-preprocessing cae-readdressing |

**Usage Guidelines**

Use this command to enable CAE re-addressing by enabling the ACS to re-address video requests to the CAEs in the CAE group.

**Examples**

The following command enables CAE re-addressing:

`video optimization-preprocessing cae-readdressing`
video pacing by-policing

This command allows you to enable the video pacing feature.

---

**Important**

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

---

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

- `active-charging service service_name > charging-action charging_action_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name{config-charging-action}#
```

**Syntax Description**

```
[ default | no ] video pacing by-policing [ initial-burst-duration value | normal-burst-duration value ][ -noconfirm ]
```

- **default**
  
  Sets video pacing by-policing to its default value, which is the same as `[ no ]`.

- **no**
  
  Deletes the video pacing by-policing settings and disables video pacing if previously configured.

**video pacing by-policing**

Enables the video pacing feature. When enabled, video pacing is applied per TCP video flow. The command syntax `by-policing` enables pacing enforcement by the policing method, which is the available method for this software release.

**initial-burst-duration value**

Specifies the duration, in seconds, for the allowed initial burst of video content. Note that the initial burst is configured in terms of time, so that for video files with different encoding bit rates, the amount of bytes allowed without enforcing pacing gets adjusted accordingly. The amount of bytes allowed is calculated by `(video encoding rate * initial-burst-duration)`.
value must be an integer between 1 and 30.
Default: 10 seconds

normal-burst-duration value
Specifies the duration, in seconds, for the allowed normal burst of video content after the initial burst is completed. Like the initial burst, the normal burst is also configured in terms of time, so that for video files with different encoding bit rates, the amount of bytes allowed without enforcing pacing gets adjusted accordingly. The amount of bytes allowed is calculated by (video encoding rate * normal-burst-duration).
value must be an integer between 1 and 30.
Default: 3 seconds

-noconfirm
Specifies that the command must execute without prompting for confirmation.

Usage Guidelines
Use this command to enable video pacing by policing.

Examples
The following command enables video pacing by policing with an initial burst duration of 15 seconds and a normal burst duration of 3 seconds:
video pacing by-policing initial-burst-duration 15 normal-burst-duration 3
xheader-insert

This command allows you to specify the extension-header (x-header) format whose fields have to be inserted in HTTP request packets and HTTP response packets.

**Important**

This command is license dependent. For more information please contact your Cisco account representative.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax Description**

```
xheader-insert xheader-format xheader_format_name [ encryption rc4md5 | encrypted | key key ] [ first-request-only ] [ msg-type { response-only | request-and-response } ] [ -noconfirm ]

no
```

Removes previously configured x-header format name.

```
xheader-format xheader_format_name
```

Enables x-header mode configuration, and specifies the x-header format whose fields are to be inserted in the packets.

`xheader_format_name` must be the name of an x-header format, and must be an alphanumeric string of 1 through 63 characters.

```
encryption rc4md5 | encrypted | key key
```

If the x-header format has any encrypted fields defined, specifies to use RC4MD5 encryption.

After configuring this option, the fields in xheader format having "encrypt" enabled will be encrypted as follows:

1. The MD5 hash of the configure key will be calculated.
2. This MD5 hash will be used as a key for RC4 encryption.
This encrypted value will be base64 encoded to get the final X-header value. The final inserted X-header will be X-alias: base64(RC4(MD5(key),MSISDN)).

In the default case, if encryption is not enabled as above, the plain text value of the xheader field will be inserted.

Note that if the value of the key is changed on the fly, it will take effect only in case of new calls. Also, if the per rulebase RSA encryption is also enabled in the same config, per charging-action RC4MD5 encryption will take precedence over it.

`key` specifies the key as an alphanumeric string of 8 through 15 characters.

`encryption` specifies use of encryption.

The `key` can be configured either as plain text or encrypted. However, in the output of the `show configuration` command it will always be displayed as encrypted. And, in the output of the `show configuration showsecrets` command it will be displayed as plain text.

`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.

`msg-type { response-only | request-and-response }`

Specifies the extension-header (x-header) format whose fields have to be inserted in HTTP Request and Response packets.

- **response-only**: X-header will be inserted in HTTP Response packets with specified x-header format.
- **request-and-response**: X-header will be inserted in both HTTP Request and Response packets with same x-header format.

`-noconfirm`

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

### Usage Guidelines

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 and HTTP response packets.

Also, see the `xheader-format` command in the ACS Configuration Mode Commands and ACS X-header Format Configuration Mode Commands chapters.

### Examples

The following command enables x-header mode, and specifies the x-header format name as `test12` for Request message:

```
xheader-insert xheader-format test12
```

The following command sets the x-header format name `format1` for both Request and Response messages:

```
xheader-insert xheader-format format1 msg-type request-and-response
```
ACS Configuration Mode Commands

The ACS Configuration Mode is used to manage active charging service (ACS)/enhanced charging service (ECS) 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.

Important
In this release only one active charging service can be configured per system.

Command Modes
Exec > ACS Configuration

active-chargingservice service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

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

- accelerate-flow, page 369
- access-ruledef, page 370
- bandwidth-policy, page 372
- buffering-limit, page 374
- charging-action, page 376
- check-point accounting, page 378
- content-filtering category match-method, page 380
- content-filtering category policy-id, page 381
- credit-control, page 383
- diameter credit-control, page 385
• edr-format, page 386
• edr-ipproto-port-map, page 388
• edr-udr-flow-control, page 389
• end, page 390
• exit, page 391
• fair-usage deact-margin, page 392
• fair-usage tcp-proxy, page 394
• fair-usage threshold-percent, page 396
• firewall dos-protection flooding, page 398
• firewall dos-protection ip-sweep, page 400
• firewall flooding, page 402
• firewall flow-recovery, page 403
• firewall icmp-destination-unreachable-message-threshold, page 405
• firewall license, page 406
• firewall max-ip-packet-size, page 407
• firewall mime-flood, page 408
• firewall nat-alg, page 409
• firewall no-ruledef-matches, page 411
• firewall port-scan, page 412
• firewall protect-servers, page 414
• firewall ruledef, page 416
• firewall tcp-syn-flood-intercept, page 418
• firewall track-list, page 419
• fw-and-nat action, page 421
• fw-and-nat policy, page 423
• group-of-objects, page 425
• group-of-prefixed-urls, page 427
• group-of-ruledefs, page 429
• h323 time-to-live, page 431
• h323 timeout, page 432
• h323 tpkt, page 434
• h323 version, page 435
• host-pool, page 436
• idle-timeout, page 438
• imsi-pool, page 440
• ip dns-learnt-entries, page 442
• ip max-fragments, page 444
• label content-id, page 445
• nat allocation-failure, page 446
• nat allocation-in-progress, page 447
• nat ip downlink reassembly-timeout, page 449
• nat tcp-2msl-timeout, page 450
• nat unsolicited-pkts, page 451
• p2p-ads-group, page 453
• p2p-detection attribute, page 455
• p2p-detection behavioral, page 457
• p2p-detection ecs-analysis, page 459
• p2p-detection protocol, page 461
• packet-filter, page 483
• passive-mode, page 485
• pcp-service, page 486
• policy-control bearer-bw-limit, page 488
• policy-control bind-default-bearer, page 489
• policy-control burst-size, page 491
• policy-control charging-action-override, page 492
• policy-control charging-rule-base-name, page 493
• policy-control dynamic-rule-limit, page 495
• policy-control l7-dynamic-rules, page 496
• policy-control retransmissions-counted, page 498
• policy-control update-default-bearer, page 499
• port-map, page 501
• qos-group-of-ruledefs, page 503
• radio-congestion, page 505
• readdress-server-list, page 507
• redirect user-agent, page 509
• rulebase, page 510
• rulebase-list, page 512
• ruledef, page 514
• service-schema, page 516
• sip advanced, page 518
• statistics-collection, page 519
• subs-class, page 521
• subscriber-base, page 522
• system-limit l4-flows, page 523
• tethering-database, page 525
• tethering-detection, page 527
• timedef, page 528
• tpo policy, page 530
• tpo profile, page 531
• trigger-action, page 532
• trigger-condition, page 534
• udr-format, page 536
• url-blacklisting match-method, page 538
• xheader-format, page 540
accelerate-flow

This command allows you to create/configure/delete Flow Aware Packet Acceleration (FAPA) feature.

Product
- GGSN
- P-GW
- PDSN
- S-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs)#

Syntax Description

| no | accelerate-flow |

- no
  If previously configured, disables the feature.

- accelerate-flow
  Enables and configures the FAPA feature.

Usage Guidelines
Use this command to create/configure/delete the FAPA feature.

Important
Accelerated ECS Packet feature will be supported when TRM FastPath is enabled on the Rulebase.

Examples
The following command enables the FAPA feature and enters the FAPA or accelerate-flow mode:
accelerate-flow
access-ruledef

This command allows you to create/configure/delete access rule definitions (ruledefs).

---

Important

This command is available only in StarOS 8.1 and in StarOS 9.0 and later releases, and must be used to configure the Policy-based Stateful Firewall and NAT features.

---

Product

NAT
PSF
SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs) #

Syntax Description

access-ruledef access_ruledef_name [-noconfirm]
no access-ruledef access_ruledef_name

no

If previously configured, deletes the specified access ruledef.

access_ruledef_name

Specifies the access ruledef to add/configure/delete.

access_ruledef_name must be the name of an access ruledef, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each access ruledef must have a unique name.

If the named access ruledef does not exist, it is created, and the CLI mode changes to the Firewall-and-NAT Access Ruledef Configuration Mode wherein the ruledef can be configured.

If the named access ruledef already exists, the CLI mode changes to the Firewall-and-NAT Access Ruledef Configuration Mode for that access ruledef.
Usage Guidelines

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 access/firewall, routing, and charging ruledefs configured in the active charging service must all have unique names.

Important

An access ruledef can be referenced by multiple Stateful Firewall rulebases.

Important

Access ruledefs are different from ACS ruledefs.

On entering this command, the CLI prompt changes to:

[context_name] hostname(config-acs-fw-ruledef)#

Also see the Firewall-and-NAT Access Ruledef Configuration Mode Commands chapter.

Examples

The following command creates an access ruledef named ruledef1, and enters the Firewall-and-NAT Access Ruledef Configuration Mode:

access-ruledef ruledef1
bandwidth-policy

This command allows you to create/configure/delete bandwidth policies.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs)#

Syntax Description
bandwidth-policy bandwidth_policy_name [ -noconfirm ]
no bandwidth-policy bandwidth_policy_name

no
If previously configured, deletes the specified bandwidth policy from the active charging service.

bandwidth_policy_name
Specifies the bandwidth policy to add/configure/delete.

bandwidth_policy_name must be the name of a bandwidth policy, and must be an alphanumeric string of 1 through 63 characters. Each bandwidth policy must have a unique name.

If the named bandwidth policy does not exist, it is created, and the CLI mode changes to the ACS Bandwidth Policy Configuration Mode wherein the bandwidth policy can be configured.

If the named bandwidth policy already exists, the CLI mode changes to the ACS Bandwidth Policy Configuration Mode for that bandwidth policy.

-noconfirm
Specifies that the command must execute without prompting for confirmation.

Usage Guidelines
Use this command to create/configure/delete a bandwidth policy.

In 12.3 and earlier releases, a maximum of 64 bandwidth policies can be configured.

In 14.0 and later releases, a maximum of 256 bandwidth policies can be configured.
On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-bandwidth-policy)#
```

Also see the *ACS Bandwidth Policy Configuration Mode Commands* chapter.

**Examples**

The following command creates a bandwidth policy named *test73*, and enters the ACS Bandwidth Policy Configuration Mode:

```
bandwidth-policy test73
```
buffering-limit

This command allows you to configure packet buffering limits.

Product  ACS

Privilege  Security Administrator, Administrator

Command Modes  Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax Description  buffering-limit { flow-max-packets flow_max_packets | subscriber-max-packets subscriber_max_packets }

{ default | no } buffering-limit { flow-max-packets | subscriber-max-packets }

default

Configures this command with its default setting.
Default: In 14.0 and earlier releases, no limit, other than the maximum amount of available memory.
Default: In 14.1 and later releases, 255

no

Disables the buffering limit configuration.

flow-max-packets flow_max_packets

Specifies the maximum number of packets that can be buffered per flow.
flow_max_packets must be an integer from 1 through 255.

subscriber-max-packets subscriber_max_packets

Specifies the maximum number of packets that can be buffered per subscriber.
subscriber_max_packets must be an integer from 1 through 255.
Usage Guidelines

Use this command to configure the limits for buffering packets sent by a subscriber, while 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.

Examples

The following command sets the buffering limit per flow to 55:

```
buffering-limit flow-max-packets 55
```
charging-action

This command allows you to create/configure/delete ACS charging actions.

A maximum of 2048 charging actions can be configured in the active charging service.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-chargingservice service_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs)#

Syntax Description

[ no ] charging-action charging_action_name [ -noconfirm ]

no

If previously configured, deletes the specified charging action from the active charging service.

charging_action_name

Specifies the charging action to add/configure/delete.

charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters and can contain punctuation characters. Each charging action must have a unique name.

If the named charging action does not exist, it is created, and the CLI mode changes to the ACS Charging Action Configuration Mode wherein the charging action can be configured.

If the named charging action already exists, the CLI mode changes to the ACS Charging Action Configuration Mode for that charging action.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete an ACS charging action.
A charging action represents actions to be taken when a configured rule is matched. Actions could range from generating an accounting record (for example, 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).

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-charging-action)#
```

Also see the ACS Charging Action Configuration Mode Commands chapter.

**Examples**

The following command creates a charging action named *action123* and changes to the ACS Charging Action Configuration Mode:

```
charging-action action123
```
check-point accounting

This command configures micro checkpoint syncup timer for ICSR and Session Recovery for Rf-Gy synchronization.

Product

- GGSN
- P-GW

Privilege

- Security Administrator
- Administrator

Command Modes

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax Description

check-point accounting sync-timer { icsr | sr } timer_value { sr | icsr } timer_value

no check-point accounting sync-timer { icsr | sr }

If the micro checkpoint syncup timer is already configured, then the no variant will delete the configuration.

sr timer_value

Configures micro check-pointing timer for Session Recovery (SR). By default, the session recovery check-pointing will be done on 8 seconds.

timer_value: Time configured will be in multiples of 2 seconds. Note that the timer value less than 4 seconds and greater than 60 seconds will not be accepted.

icsr timer_value

Configures micro check-pointing timer for ICSR. By default, the ICSR check-pointing will be done on 18 seconds.

timer_value: Time configured will be in multiples of 2 seconds. Note that the timer value less than 4 seconds and greater than 60 seconds will not be accepted.

Usage Guidelines

Use this command to configure micro checkpoint syncup timer for ICSR and Session Recovery. Micro Checkpoint Sync-up timer is an internal timer utilized by Rf and Gy modules to check point corresponding billing information.
Releases prior to 17.0, micro checkpoint sync-up timer was hardcoded with a value of 18 seconds for ICSR and 8 seconds for Session Recovery (SR). In 17.0 and later releases, the micro checkpoint sync-up timer is made configurable with an expectation that it be set at a value as low as 4 seconds. The timer value is reduced to ensure the accurate billing information during the ICSR or SR switchover event.

This CLI is available at both active charging service level and rulebase level. If the timer value is configured at both service and rulebase level, then the service level value will be overridden with rulebase level values.

This feature provides the operator with the flexibility to provision timer for accurate billing information in case of session recovery or ICSR switchover. However, this is a performance impacting feature and the impact of the micro checkpoint sync timer reduction needs to be carefully considered by the operator before provisioning a lower value.

**Examples**

The following command configures the micro checkpoint syncup timer for Session Recovery as 8 seconds:

```
check-point accounting sync-timer sr 8
```
content-filtering category match-method

This command allows you to specify the match method to look up URLs in the Category-based Content Filtering database.

Product
CF

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration
active-charging service service_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs) #

Syntax Description
content-filtering category match-method { exact | generic }
default content-filtering category match-method

default
Configures this command with its default setting.
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, and rollback algorithms are applied to URLs during look up. URLs are rated on generic match with URLs present in the Category-based Content Filtering database.

Usage Guidelines
Use this command to set the match method to look up URLs in the Category-based Content Filtering database.

Examples
The following command sets the exact-match method to look up URLs in the Category-based Content Filtering database:
content-filtering category match-method exact
content-filtering category policy-id

This command allows you to create/configure/delete Content Filtering Category Policies for Category-based Content Filtering support.

Important
A maximum of 64 Content Filtering Category Policies can be configured in the active charging service.

Product
CF

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs) #

Syntax Description
content-filtering category policy-id cf_policy_id [ description [ description_string ] ] [ -noconfirm ]
no content-filtering category policy-id cf_policy_id

no
If previously configured, deletes the specified Content Filtering Category Policy from the active charging service.

cf_policy_id
Specifies the Content Filtering Category Policy ID to add/configure/delete.
cf_policy_id must be an integer from 1 through 4294967295.
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 for that policy.

description [ description_string ]
Specifies a description for the Content Filtering Category Policy.
description_string must be an alphanumeric string of 1 through 31 characters.
Note that both **description** and **description_string** are optional. 

"**description** description_string" 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 Guidelines**

Use this command to create/configure/delete a Content Filtering Category Policy. 

On entering this command, the CLI prompt changes to: 

```
[context_name]hostname(config-acs-content-filtering-policy)#
```

Also see the **Content Filtering Policy Configuration Mode Commands** chapter.

**Examples**

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 allows you to enable/disable Prepaid Credit Control Configuration Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)>
```

**Syntax Description**

```
[ no ] credit-control [ group cc_group_name ]
```

- **no**
  Disables the specified Prepaid Credit Control Application configuration.

- **group cc_group_name**
  
  **Important**
  This option is only available in StarOS 8.1 and later releases.

  Specifies the credit control group to add/configure/delete.

  `cc_group_name` must be the name of a credit control group, and must be an alphanumeric string of 1 through 63 characters. Each credit control group must have a unique name.

  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 for that credit control group.

  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.
**Important**

ICSR support for credit-control group is limited to a maximum of three bearers (one default and two dedicated bearers).

**Usage Guidelines**

Use this command to enable/disable Prepaid Credit Control Configuration for RADIUS/Diameter charging mode.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-dcca)#
```

Also see the *Credit Control Configuration Mode Commands* chapter.

**Examples**

The following command enables prepaid credit control accounting to use RADIUS and/or Diameter interface mode.

```
credit-control
```
diameter credit-control

This command has been deprecated, and is replaced by the credit-control, on page 383 command.
edr-format

This command allows you to create/configure/delete ACS Event Data Record (EDR) formats.

Important

A maximum of 256 EDR plus UDR formats can be configured in the active charging service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax Description

edr-format edr_format_name [ -noconfirm ]

no edr-format edr_format_name

no

If previously configured, deletes the specified EDR format from the active charging service.

edr_format_name

Specifies the EDR format to add/configure/delete.

edr_format_name must be an alphanumeric string of 1 through 63 characters. Each EDR format must have a unique name.

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 for that EDR format.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete an EDR format.
On entering this command, the CLI prompt changes to:
[context_name]hostname(config-acr-edr)#

Also see the EDR Format Configuration Mode Commands chapter.

**Examples**

The following command creates an EDR format named *edr_format1*, and enters the EDR Format Configuration Mode:

```
edr-format edr_format1
```
edr-ipproto-port-map

This command enables IP protocol and server port mapping for Event Data Records (EDR).

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs)#

Syntax Description

| default | no | edr-ipproto-port-map

default

Configures this command with its default setting.

Default: Disabled

no

If previously enabled, disables the IP protocol and server port mapping for EDR.

Usage Guidelines

Use this command to enable IP protocol and server port mapping for EDR. As part of EDR generation, packets can be mapped based on IP header protocol and Transport Header Port. Generating statistics based on IP Protocol and Transport Port number is an added advantage for offline packet analysis.
edr-udr-flow-control

This command allows you to enable/disable flow control between Session Managers (SessMgrs) and the CDRMOD process.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax Description

edr-udr-flow-control [ unsent-queue-size unsent_queue_size ]
{ default | no } edr-udr-flow-control

no
If previously enabled, disables the flow control configuration.

default
Configures this command with its default setting.
Default: Flow control is enabled; unsent-queue-size: 375

unsent-queue-size unsent_queue_size
Specifies the flow control unsent queue size at Session Manager (SessMgr) level.
unsent_queue_size must be an integer from 1 through 2500.

Usage Guidelines

Use this command to enable Flow Control between SessMgr and the CDRMOD process, and configure the unsent queue size.

Examples

The following command enable Flow Control between SessMgrs and the CDRMOD process, and configure the unsent queue size to 1000:

edr-udr-flow-control unsent-queue-size 1000
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

end

Usage Guidelines

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 Description**
exit

**Usage Guidelines**
Use this command to return to the parent configuration mode.
**fair-usage deact-margin**

This command allows you to configure the deactivate margin for the Fair Usage feature.

---

**Important**

In release 17.0, this command has been deprecated.

---

**Product**

ACS  
ADC  
CF  
PSF  
NAT  

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

---

**Syntax Description**

`fair-usage deact-margin deactivate_margin`

`default` *fair-usage deact-margin*

- **default**
  
  Configures this command with its default setting.
  
  Default: 5 percent

- **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.
Usage Guidelines

Use this command to configure when to disable the Fair Usage feature, which enables SessMgr instance-level load balancing for in-line service features, and resource usage control for subscribers. For additional information, refer to the feature description in the Enhanced Charging Service Administration Guide.

Examples

The following command configures the deactivate margin to disable Fair Usage monitoring to 10% below the session resource usage threshold (65%):

```
fair-usage deact-margin 10
```
fair-usage tcp-proxy

This command allows you to configure the maximum number of flows for which TCP Proxy can be used per subscriber, and what portion of ECS memory should be reserved for TCP Proxy flows.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax Description

fair-usage tcp-proxy { max-flows-per-subscriber max_flows_subscriber | memory-share memory_share }
default fair-usage [ max-flows-per-subscriber | memory-share ]

default

Configures this command with its default setting.

max-flows-per-subscriber max_flows_subscriber

Specifies the maximum number of flows for which TCP Proxy can be used per subscriber. This limit is per Session Manager.

max_flows_subscriber must be an integer from 1 through 1000.

Default: 5

memory-share memory_share

Specifies what portion of ECS memory should be reserved for TCP Proxy flows.

memory_share is a percentage value, and must be an integer from 1 through 100.

Default: 10%

Usage Guidelines

Use this command to configure the maximum number of flows for which TCP Proxy can be used for a subscriber, and what portion of ECS memory should be reserved for TCP Proxy flows.
### Examples

The following command configures 100 as the maximum number of flows for which TCP Proxy can be enabled for the subscriber:

```
fair-usage tcp-proxy max-flows-per-subscriber 100
```
**fair-usage threshold-percent**

This command allows you to configure the usage threshold to start Fair Usage monitoring.

---

**Important**

In release 17.0, this command has been deprecated.

---

**Product**

- ACS
- ADC
- CF
- PSF
- NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

- Exec > ACS Configuration

**Syntax Description**

```
fair-usage threshold-percent usage_threshold
default fair-usage threshold-percent
```

- **default**
  
  Configures this command with its default setting.
  
  Default: 50 percent

- **usage_threshold**
  
  Specifies the threshold to start Fair Usage monitoring. Until the credit usage hits this threshold, all session resource allocation is allowed. On crossing this threshold, any new resource allocation request is evaluated before being allowed or denied.

  Usage threshold is a percentage value, and must be an integer from 1 through 100.
Usage Guidelines

Use this command to configure the threshold to enable the Fair Usage feature, which enables SessMgr instance-level load balancing for in-line service features, and resource usage control for subscribers. For additional information, refer to the feature description in the *Enhanced Charging Service Administration Guide*.

Examples

The following command enables the Fair Usage feature, and configures the session resource usage threshold to start Fair Usage monitoring to 75%:

```
fair-usage threshold-percent 75
```
firewall dos-protection flooding

This command is configured to protect servers from mobile subscribers in the uplink direction.

Important

In StarOS 17.0 and later releases, the uplink flooding feature is not enabled in the ACS Configuration mode, and must be enabled in the Firewall-and-NAT Policy Configuration mode. Hence, this command is no longer supported and left in place for backward compatibility.

Product

PSF
NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax Description

firewall dos-protection flooding { { icmp | tcp-syn | udp } protect-servers { all | host-pool hostpool_name } packet limit packet_limit | inactivity-timeout timeout | uplink-sample-interval interval } default firewall dos-protection flooding { icmp | tcp-syn | udp | inactivity-timeout | uplink-sample-interval } no firewall dos-protection flooding { icmp | tcp-syn | udp }

no

Disables Stateful Firewall protection for subscribers against the specified Denial of Service (DoS) attack(s).

default

Disables Stateful Firewall protection for subscribers against all DoS attacks.

flooding { icmp | tcp-syn | udp } protect-servers { all | host-pool hostpool_name }

Enables protection against the specified flooding attack:

• icmp: Enables ICMP uplink flooding protection.

• tcp-syn: Enables TCP Syn uplink flooding protection.
- **udp**: Enables UDP uplink flooding protection.

**all**: Enables protection for all the servers.

**host-pool** *hostpool_name*: Specifies the name of the host pool. *hostpool_name* must be an alphanumeric string of 1 through 63 characters.

**packet limit** *packet_limit*

Specifies the maximum number of packets allowed during a sampling interval. *packet_limit* must be an integer from 1 through 4294967295.

Default: 1000 packets per sampling interval for all protocols.

**inactivity-timeout** *inactivity_timeout*

Specifies the inactivity timeout period, in seconds. This allows flooding traffic if the destination is inactive for more than the configured period. *inactivity_timeout* must be an integer from 1 through 4294967295.

Default: 300 seconds

**uplink-sample-interval** *interval*

Specifies the uplink sampling interval, in seconds. The maximum sampling-interval configurable is 60 seconds. *interval* must be an integer from 1 through 60.

Default: 1 second

**Usage Guidelines**

Use this command to enable Stateful Firewall protection from different types of DoS attacks for all servers or for those servers mentioned in the host pool. This allows users to safeguard their own servers and other hosts.

DoS attacks are also detected in the downlink direction. The `firewall dos-protection` command must be configured in the FW-and-NAT Policy Configuration mode.

**Examples**

The following command enables ICMP uplink protection for all servers with packet limit set to 10:

```
firwall dos-protection flooding icmp protect-servers all packet limit 10
```
**firewall dos-protection ip-sweep**

This command is configured to detect Source IP-based flooding attacks in the uplink direction.

---

**Important**

In StarOS 17.0 and later releases, the IPsweep feature is not enabled in the ACS Configuration mode, and must be enabled in the Firewall-and-NAT Policy Configuration mode. Hence, this command is no longer supported and left in place for backward compatibility.

---

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

**active-charging service service_name**

Entering the above command sequence results in the following prompt:

[local] *host_name*(config-acs)#

**Syntax Description**

firewall dos-protection ip-sweep { icmp | tcp-syn | udp } protect-servers { all | host-pool hostpool_name } packet limit packet_limit | downlink-server-limit server_limit | inactivity-timeout timeout | sample-interval interval }

default firewall dos-protection ip-sweep { downlink-server-limit | icmp | inactivity-timeout | sample-interval | tcp-syn | udp }

no firewall dos-protection ip-sweep { icmp | tcp-syn | udp }

default

Disables Stateful Firewall protection for subscribers against all DoS attacks.

no

Disables Stateful Firewall protection for subscribers against the specified Denial of Service (DoS) attack(s).

ip-sweep { icmp | tcp-syn | udp } protect-servers { all | host-pool hostpool_name }

Enables protection against the specified flooding attack:

- **icmp**: Enables source IP-based flood attack detection for ICMP.
- **tcp-syn**: Enables source IP-based flood attack detection for TCP-SYN.
- **udp**: Enables source IP-based flood attack detection for UDP.
**Usage Guidelines**

Use this command to enable or disable IP Sweep Protection in the uplink direction for mobile subscribers and internet hosts on a per protocol basis. The purpose of the Uplink IP Sweep protection is to check whether a particular source IP address is generating more flows per sample interval than is permitted. If so, the first packets that come after the maximum packet limit during the particular time interval will be dropped.

IP Sweep attacks are also detected in the downlink direction. The `firewall dos-protection ip-sweep` command must be configured in the FW-and-NAT Policy Configuration mode. The configuration values for packet limit and sampling interval are common for both uplink and downlink.

**Examples**

The following command enables ICMP uplink protection for all servers with packet limit set to 30:

```
firwall dos-protection ip-sweep icmp protect-servers all packet limit 30
```
firewall flooding

**Description** In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS 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 ACS Rulebase Configuration Mode.
**firewall flow-recovery**

This command allows you to configure the Stateful Firewall's Flow Recovery feature.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**

```
firewall flow-recovery { { downlink [ [ timeout timeout ] [ no-flow-creation ] + ] } | { uplink [ timeout timeout ] } } 
{ default | no } firewall flow-recovery { downlink | uplink }
```

- **default**
  Configures this command with its default setting.
  Default: Downlink and uplink flow recovery enabled, 300 seconds

- **no**
  Disables the flow recovery configuration.

- **downlink** | **uplink**
  Specifies the packets:
  - **downlink**: Enables flow recovery for packets from the downlink direction.
  - **uplink**: Enables flow recovery for packets from the 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 Guidelines**

Use this command to configure Stateful Firewall Flow Recovery feature.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT flows will not be recovered.</td>
</tr>
</tbody>
</table>

**Examples**

The following command configures Stateful Firewall Flow Recovery for packets in downlink direction with a timeout setting of 600 seconds:

```
firewall flow-recovery downlink timeout 600
```
firewall icmp-destination-unreachable-message-threshold

**Description** In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS 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 ACS Rulebase Configuration Mode.
**firewall license**

This command allows you to configure the license related parameters for Stateful Firewall.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**
```
firewall license exceed-action { disable-feature | drop-call | ignore }
```

```
exceed-action { disable-feature | drop-call | ignore }
```

Configures one of the following parameters when license is exceeded.

- **disable-feature**: Disables the service when license is exceeded.
- **drop-call**: Drops the call if call fails to get a Stateful Firewall license.
- **ignore**: Continues using the Stateful Firewall license even if license is exceeded. This is the default behavior.

**Usage Guidelines**
Use this command to configure the license related parameters for Stateful Firewall when license is exceeded.
**firewall max-ip-packet-size**

**Description** In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS 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 ACS Rulebase Configuration Mode.
firewall mime-flood

**Description** In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS 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 ACS Rulebase Configuration Mode.
firewall nat-alg

This command enables/disables Network Address Translation (NAT) Application Level Gateways (ALGs).

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs)#
```

**Syntax Description**

```
[ default | no ] firewall nat-alg { all | ftp | h323 | pptp | rtsp | sip } [ ipv4-and-ipv6 | ipv4-only | ipv6-only ]
```

**default**
Configures this command with the default setting for the specified parameter.

Default:
- **ftp**: Enabled
- **h323**: Enabled
- **pptp**: Disabled
- **rtsp**: Disabled
- **sip**: Disabled

**no**
Disables all/ or the specified NAT ALG configuration. When disabled, the ALG(s) will not do any payload translation for NATd calls.

```
all | ftp | h323 | 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.
• **h323**: Enables/disables H323 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.

**ipv4-and-ipv6 | ipv4-only | ipv6-only**

Specifies to enable/disable NAT44/NAT64 ALG.

• **ipv4-and-ipv6**: Enables both NAT44 and NAT64 ALGs.
• **ipv4-only**: Enables only NAT44 ALG.
• **ipv6-only**: Enables only NAT64 ALG.

**Usage Guidelines**

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.

**Examples**

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 H.323, PPTP, RTSP, and SIP NAT ALGs:
```
default firewall nat-alg all
```
firewall no-ruledef-matches

Description In StarOS 8.1 and later releases, this command is available in the ACS Rulebase Configuration Mode.
**firewall port-scan**

This command allows you to configure Stateful Firewall's Port Scan Detection algorithm.

**Product**  
PSF

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration  
```
active-charging service service_name
```
Entering the above command sequence results in the following prompt:
```
[local]host_name(config-acs)#
```

**Syntax Description**
```
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 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
```
Confirms this command with its default setting.

**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 and response-timeout period.

- **tcp**: Specifies response timeout for TCP.
  
  *response_timeout* must be an integer from 1 through 30.

- **udp**: Specifies response timeout for UDP.
  
  *response_timeout* must be an integer from 1 through 60.

Default: 3 seconds

**scanner-policy** { block inactivity-timeout *inactivity_timeout* | log-only }

Specifies how to treat packets from a source address that has been detected as a scanner.

- **block inactivity-timeout** *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.

  *inactivity_timeout* specifies the scanner inactivity timeout period, in seconds, and must be an integer from 1 through 4294967295.

- **log-only**: Specifies logging scanner information without blocking scanner traffic.

Default: **log-only**

**Usage Guidelines**

Use this command to configure the Stateful Firewall Port Scan Detection algorithm enabled by the **firewall dos-protection port-scan** CLI command.

This protection tracks all uplink source addresses, and the packets they initiate towards all subscribers that have this protection enabled.

**Examples**

The following command configures the Stateful Firewall Port Scan inactivity timeout setting to 900 seconds:

```
firewall port-scan inactivity-timeout 900
```
**firewall protect-servers**

This command is configured to protect ISP servers from mobile space devices.

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

*active-charging service* service_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs)#

**Syntax Description**

`firewall protect-servers { all | host-pool hostpool_name } policy policy_name { default | no } firewall protect-servers`

**default**

Configures this command with its default setting.

**no**

Disables protection of the servers.

**all**

Configured to protect all servers from attacking mobile nodes.

**host-pool hostpool_name**

Specifies the name of the host pool where all servers in that host pool need to be protected.

*hostpool_name* must be an alphanumeric string of 1 through 63 characters.

**policy policy_name**

Specifies the Firewall-and-NAT policy to be applied to packets that are destined to the IPs mentioned in the host pool.

*policy_name* must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters.
Usage Guidelines

Use this command to protect all ISP servers or specific ISP servers from mobile space devices. All the uplink packets will be inspected, and the action will be taken based on the configuration in Firewall-and-NAT policy. Uplink protection can be enabled or disabled based on the server IP of the packet.

Examples

The following command is configured to protect all servers within a Firewall-and-NAT policy named test123:

```
firewall protect-servers all policy test123
```
firewall ruledef

This command allows you to create/configure/delete Stateful Firewall ruledefs.

Important
This command is available only in StarOS 8.1. This command must be used to configure the Rulebase-based Stateful Firewall and NAT features.

Product
PSF

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration

active-charging service service_name
Entering the above command sequence results in the following prompt:
[local]host_name(config-acsf)#

Syntax Description
firewall ruledef firewall_ruledef_name [-noconfirm]
no firewall ruledef firewall_ruledef_name

no
If previously configured, deletes the specified Stateful Firewall ruledef from the active charging service.

firewall_ruledef_name
Specifies the Stateful Firewall ruledef to add/configure/delete.
firewall_ruledef_name must be the name of a Stateful Firewall ruledef, and must be an alphanumeric string of 1 through 63 characters and can contain punctuation characters. Each ruledef must have a unique name.
If the named 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 Stateful Firewall ruledef already exists, the CLI mode changes to the Firewall Ruledef Configuration Mode for that ruledef.

-noconfirm
Specifies that the command must execute without prompting for confirmation.
Usage Guidelines

Use this command to create/configure/delete a Stateful Firewall ruledef. A Stateful Firewall ruledef contains different conditions to permit, drop, or reject a packet/connection/traffic based on one or more parameters. The ruledef name must be unique within the active charging service. Host pool, port map, IMSI pool, and Stateful Firewall, routing, and charging ruledefs must have unique names.

A Stateful Firewall ruledef can be referenced by multiple Stateful Firewall rulebases.

Important

The Stateful Firewall ruledefs are different from the ACS ruledefs.

Also see the Firewall-and-NAT Access Ruledef Configuration Mode Commands chapter.

Examples

The following command creates a Stateful Firewall ruledef named `fw_ruledef1`, and enters the Firewall Ruledef Configuration Mode:

```
firewall ruledef fw_ruledef1
```
firewall tcp-syn-flood-intercept

**Description** In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS 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 ACS Rulebase Configuration Mode.
firewall track-list

This command allows you to configure the maximum number of server IP addresses to be tracked that are involved in any kind of denial-of-service (DoS) attacks.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**

```
firewall track-list attacking-servers no_of_servers
{ default | no } firewall track-list attacking-servers
```

- **default**
  Configures this command with its default setting.
  Default: 10 servers

- **no**

**Important**

This command variant is available only in StarOS 8.3 and later releases.

If previously configured, deletes the configuration from the active charging service.

```
attacking-servers no_of_servers
```

Specifies the maximum number of servers to track.

*no_of_servers* must be an integer from 1 through 100.

**Usage Guidelines**

Use this command to configure the maximum number of server IP addresses to be tracked that are involved in any kind of DoS attacks.
The following command configures the maximum number of server IP addresses to be tracked that are involved in any kind of DoS attacks to 20:

```
firewall track-list attacking-servers 20
```
fw-and-nat action

This command allows you to create/configure/delete Firewall-and-NAT actions.

| Important | This command is available only in 11.0 and later releases. This command must be used to configure the Stateful Firewall and NAT Action. |

**Product**

PSF
NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

**Syntax Description**

fw-and-nat action action_name [-noconfirm]  
no fw-and-nat action action_name

- **no**
  - If previously configured, deletes the specified Firewall-and-NAT action from the active charging service.

- **action_name**
  - Specifies the Firewall-and-NAT action to add/configure/delete.

- **action_name** must be the name of a Firewall-and-NAT action, and must be an alphanumeric string of 1 through 63 characters. Each Firewall-and-NAT action must have a unique name.

- **-noconfirm**
  - Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**

Use this command to create/configure/delete a Firewall-and-NAT action.

On entering this command, the CLI prompt changes to:
Also see the *Firewall-and-NAT Action Configuration Mode Commands* chapter.

**Examples**

The following command creates a Firewall-and-NAT action named *test1*, and changes to the Firewall-and-NAT Action Configuration Mode:

`fw-and-nat action test1`
fw-and-nat policy

This command allows you to create/configure/delete Firewall-and-NAT policies.

Important
This command is available only in StarOS 8.1 and in StarOS 9.0 and later releases. This command must be used to configure the Policy-based Stateful Firewall and NAT features.

Product
PSF
NAT
SaMOG

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax Description
fw-and-nat policy policy_name [ -noconfirm ]
no fw-and-nat policy fw_nat_policy_name

no
If previously configured, deletes the specified Firewall-and-NAT policy from the active charging service.

Important
When a Firewall-and-NAT policy is deleted, for all subscribers using the policy, Stateful Firewall and NAT processing is disabled, also ACS sessions for the subscribers are dropped. In case of session recovery, the calls are recovered but with Stateful Firewall and NAT disabled.

fw_nat_policy_name
Specifies the Firewall-and-NAT policy to add/configure/delete.

fw_nat_policy_name must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters. Each Firewall-and-NAT policy must have a unique name.
**fw-and-nat policy**

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**
Use this command to create/configure/delete a Firewall-and-NAT policy.
On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-fw-and-nat-policy)#
```

Also see the *Firewall-and-NAT Policy Configuration Mode Commands* chapter.

**Examples**
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-objects

This command allows you to create/configure/delete an ACS group-of-objects.

Important

This command is available only in StarOS 10.2 and later releases.

Important

A maximum of 16 object groups can be configured in the active charging service. And a maximum of 128 objects can be configured within each object group.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs) #

Syntax Description

group-of-objects objects_group_name [ type string [ -noconfirm ] ]

no group-of-objects objects_group_name

no

If previously configured, deletes the specified group-of-objects from the active charging service.

objects_group_name

Specifies the group-of-objects to add/configure/delete.

objects_group_name must be the name of a group-of-objects, and must be an alphanumeric string of 1 through 63 characters. Each group-of-objects must have a unique name.

If the named group-of-objects does not exist, it is created, and the CLI mode changes to the ACS Group-of-Objects Configuration Mode wherein the group can be configured.

If the named group-of-objects already exists, the CLI mode changes to the ACS Group-of-Objects Configuration Mode for that group.
**type**
Specifies the data type for the group-of-objects.

---

**Important**
"string" is the only data type supported in this release.

**string**
Specifies the data type as string.
When creating a group, specifying the data type is mandatory.
When modifying an existing group, specifying the data type is optional.

**-noconfirm**
Specifies that the command must execute without prompting for confirmation.

---

**Usage Guidelines**
Use this command to create/configure/delete a group-of-objects.
On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-acs-group-of-objects)#
```

Also see the ACS Group-of-Objects Configuration Mode Commands chapter.

**Examples**
The following command creates a group-of-objects named *test4* with the data type string, and enters the ACS Group-of-Objects Configuration Mode:

```
group-of-objects test4 type string
```
**group-of-prefixed-urls**

This command allows you to create/configure/delete an ACS group-of-prefixed-URLs.

---

**Important**

This command is customer specific. For more information contact your Cisco account representative.

---

**Important**

A maximum of 64 group-of-prefixed-URL groups can be configured in the active charging service.

---

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**

`group-of-prefixed-urls prefixed_urls_group_name [ -noconfirm ]`

`no group-of-prefixed-urls prefixed_urls_group_name`

- **no**
  
  If previously configured, deletes the specified group-of-prefixed-urls from the active charging service.

`prefixed_urls_group_name`

Specifying the group-of-prefixed-urls to add/configure/delete.

`prefixed_urls_group_name` must be the name of a group-of-prefixed-urls, and must be an alphanumeric string of 1 through 63 characters. Each group-of-prefixed-urls must have a unique name.

If the named group-of-prefixed-urls does not exist, it is created, and the CLI mode changes to the ACS Group-of-Prefixed-URLs Configuration Mode wherein the group can be configured.

If the named group-of-prefixed-urls already exists, the CLI mode changes to the ACS Group-of-Prefixed-URLs Configuration Mode for that group.
-noconfirm
Specifies that the command must execute without prompting for confirmation.

Usage Guidelines
Use this command to create/configure/delete a group-of-prefixed-URLs.
On entering this command, the CLI prompt changes to:
[context_name]hostname(config-acs-grp-of-prefixed-urls)#
Also see the ACS Group-of-Prefixed-URLs Configuration Mode Commands chapter.

Examples
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 allows you to create/configure/delete an ACS group-of-ruledefs.

**Important**

In 14.1 and earlier releases, a maximum of 64 group-of-ruledefs can be configured in the active charging service. In 15.0 and later releases, a maximum of 128 group-of-ruledefs can be configured.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs) #
```

**Syntax Description**

```
group-of-ruledefs ruledefs_group_name [ -noconfirm ]
no group-of-ruledefs ruledefs_group_name
```

no

If previously configured, deletes the specified group-of-ruledefs from the active charging service.

`ruledefs_group_name`

Specifies the group-of-ruledefs to add/configure/delete.

`ruledefs_group_name` must be unique within the active charging service, and must be an alphanumeric string of 1 through 63 characters. Each group-of-ruledefs must have a unique name.

If the named group-of-ruledefs does not exist, it is created, and the CLI mode changes to the ACS Group-of-Ruledefs Configuration Mode wherein the group can be configured.

If the named group-of-ruledefs already exists, the CLI mode changes to the ACS Group-of-Ruledefs Configuration Mode for that group.

`-noconfirm`

Specifies that the command must execute without prompting for confirmation.
Usage Guidelines

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.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-group-of-ruledefs)#
```

Also see the ACS Group-of-Ruledefs Configuration Mode Commands chapter.

Examples

The following command creates a group-of-ruledefs named `group1`, and enters the ACS Group-of-Ruledefs Configuration Mode:

```
group-of-ruledefs group1
```
h323 time-to-live

This command allows you to configure the time period for which an endpoint's registration to an H.323 gatekeeper is valid.

Product
NAT

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration

active-charging service service_name
Entering the above command sequence results in the following prompt:
[local]host_name(config-acs)#

Syntax Description
h323 time-to-live timeout
default h323 time-to-live
default
Configures this command with its default setting.
Default: 3600 seconds
timeout
Specifies the timeout setting, in seconds.
timeout must be an integer from 1 through 2147483647.

Usage Guidelines
Use this command to configure the time period for which an endpoint's registration to a gatekeeper is valid.

Examples
The following command configures the time for an endpoint registration with a timeout setting of 5 seconds:
h323 time-to-live 5
h323 timeout

This command allows you to configure the timeout intervals for various H.323 requests.

Product
NAT

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration

active-charging_service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax Description
h323 timeout { admission admission_timeout | discovery discovery_timeout | location location_timeout | registration registration_timeout | unregistration unregistration_timeout }

default h323 timeout { admission | discovery | location | registration | unregistration }

default

Configures this command with the default setting for the specified parameters.

admission admission_timeout

Configures the timeout value for the admission request sent to the gatekeeper.

admission_timeout must be an integer from 1 through 20.

Default: 10 seconds

discovery discovery_timeout

Configures the timeout value for the gatekeeper request message sent to the Gatekeeper.

discovery_timeout must be an integer from 1 through 20.

Default: 10 seconds

location location_timeout

Configures the timeout value for the location request message sent to the Gatekeeper.

location_timeout must be an integer from 1 through 20.

Default: 10 seconds
registration registration_timeout
Configures the timeout value for the registration request message sent to the Gatekeeper. 
registration_timeout must be an integer from 1 through 20. 
Default: 6 seconds

unregistration unregistration_timeout
Configures the timeout value for the unregistration request message sent to the Gatekeeper. 
unregistration_timeout must be an integer from 1 through 20. 
Default: 3 seconds

Usage Guidelines
Use this command to configure the timeout interval for the various H.323 requests.

Examples
The following command configures the admission request message with a timeout value of 15 seconds: 
h323 timeout admission 15
**h323 tpkt**

This command allows you to configure the maximum size of Transport Protocol Data Unit Packets (TPKT) that the H.323 Application Layer Gateway (ALG) can handle.

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs)#
```

**Syntax Description**

```
h323 tpkt max_tpkt_size
default h323 tpkt
```

- **default**
  
  Configures this command with its default setting.
  
  Default: 2048 bytes

- **max_tpkt_size**
  
  Specifies the maximum TPKT size, in bytes.
  
  `max_tpkt_size` must be an integer from 4 through 4096.

**Usage Guidelines**

Use this command to configure the maximum packet size for the H.323 ALG.

**Examples**

The following command configures a maximum TPKT packet size of 100 bytes:

```
h323 tpkt 100
```
**h323 version**

This command allows you to configure the H.323 version number supported by an H.323 Application Layer Gateway (ALG).

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

**active-charging service service_name**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**

```
h323 version h323_version_number
default h323_version
```

- **default**
  
  Configures this command with its default setting.
  
  Default: 5

- **h323_version_number**
  
  Specifies the H.323 version number.
  
  `h323_version_number` must be an integer from 1 through 7.

**Usage Guidelines**

Use this command to configure the H.323 version number supported by the H.323 ALG.

**Examples**

The following command configures the H.323 version as 1:

```
h323 version 1
```
**host-pool**

This command allows you to create/configure/delete host pools.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs)#
```

**Syntax Description**

`host-pool host_pool_name [-noconfirm ]`

`no host-pool host_pool_name`

`no`

If previously configured, deletes the specified host pool from the active charging service.

`host_pool_name`

Specifies the host pool to add/configure/delete.

`host_pool_name` must be the name of a host pool, and must be an alphanumeric string of 1 through 63 characters and can contain punctuation characters. Each host pool must have a unique name.

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 for that host pool.

`-noconfirm`

Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**

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 configured in other ruledefs cannot be deleted.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-acs-host-pool)#
```

Also see the *ACS Host Pool Configuration Mode Commands* chapter.

**Examples**  
The following command creates a host pool named `hostpool1`, and enters the ACS Host Pool Configuration Mode:

```
host-pool hostpool1
```
idle-timeout

This command allows you to configure the maximum duration a flow can remain idle for, after which the system automatically terminates the flow.

**Product**
ACS
NAT
PSF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

**active-charging service** service_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs)#

**Syntax Description**

idle-timeout { alg-media | flow-mapping { tcp | udp | icmp | tcp [ half-open ] | udp } } idle_timeout
{ default | no } idle-timeout { alg-media | flow-mapping { tcp | udp | icmp | tcp [ half-open ] | udp } }

*default*
Configures this command with the default setting for the specified parameter.

Default:

- **alg-media**: 120 seconds
- **flow-mapping { tcp | udp }**: 300 seconds for TCP and 0 seconds for UDP
- **icmp, tcp, udp**: 300 seconds
- **tcp half-open**: 200 seconds

*no*
Disables the idle-timeout configuration for the specified flow.

**alg-media**
Configures the ALG media for the specified flow.
flow-mapping \{ tcp | udp \}

The Flow Mapping timer is an extension to the existing flow idle-timeout in ACS. This flow mapping timeout applies only for NAT enabled calls and is supported only for TCP and UDP flows. The purpose of this timer is to hold the resources (NAT IP, NAT port, Private IP NPU flow) associated with a 5-tuple flow until Mapping timeout expiry.

If the Flow Mapping timer is disabled, then the Mapping timeout will not get triggered for UDP/TCP idle timed out flows. The resources such as NAT mapping will be released along with the 5-tuple flow.

icmp

Configures the ICMP protocol for the specified flow.

tcp [ half-open ]

Configures the TCP protocol for the specified flow.

Use the half-open keyword to configure timeout interval for half-open TCP flows.

udp

Configures the UDP protocol 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 Guidelines

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 value 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 active charging service.

Examples

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 allows you to create/configure/delete International Mobile Subscriber Identity (IMSI) pools.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**

`imsi-pool imsii_pool_name | -noconfirm |`

`no imsi-pool imsii_pool_name`

- **no**
  - If previously configured, deletes the specified IMSI pool from the active charging service.

  **imsii_pool_name**
  - Specifies the IMSI pool to add/configure/delete.

  - `imsii_pool_name` must be the name of an IMSI pool, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each IMSI pool must have a unique name.

  - 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 for that IMSI pool.

  **-noconfirm**
  - Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**

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 within the service. Host pool, port map, IMSI pool, and firewall, routing, and charging rulesdefs must have unique names. A maximum of 256 IMSI pools can be created.
Important  IMSI pools configured in other ruledefs cannot be deleted.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-acs-imsi-pool)#
```

Also see the ACS IMSI Pool Configuration Mode Commands chapter.

Examples  The following command creates an IMSI pool named `imsipool1`, and enters the ACS IMSI Pool Configuration Mode:

```
imsi-pool imsipool1
```
ip dns-learnt-entries

This command allows you to configure how long to keep the snooped IPv4 addresses that were extracted from DNS responses.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

*active-charging service service_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-acs)#`

**Syntax Description**

`ip dns-learnt-entries timeout timeout_period`

`{ default | no } ip dns-learnt-entries timeout`

**default**

Configures this command with the default DNS-learnt-entries timeout setting.

Default: 300 seconds

**no**

Specifies to always use the TTL value in the DNS response, and not the timeout configured with this command.

**timeout_period**

Specifies the DNS-learnt-entries timeout period, in seconds.

`timeout_period` must be an integer from 1 through 2147483647.

**Usage Guidelines**

Use this command to configure how long to keep the snooped IPv4 addresses that were extracted from DNS responses—for the TTL specified in the DNS response, or for the time period configured with this command, if greater.

The configurable timer will be at global ECS level and shared across all IP addresses. Internally, a five-minute (300 seconds, non configurable) timer will be started whenever DNS analyzer is enabled. On timeout of this timer, all the learnt IP addresses will be checked for TTL expiry and the expired entries will be flushed.
Examples

The following command specifies to keep the snooped IPv4 addresses that were extracted from DNS responses for a time period of 900 seconds, or for the TTL value specified in the DNS response, whichever is greater:

```
ip dns-learnt-entries timeout 900
```
**ip max-fragments**

This command allows you to limit the maximum number of IPv4/IPv6 fragments per fragment chain.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

*active-charging service service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**

`ip max-fragments max_fragments`

`default ip max-fragments`

- **default**
  
  Configures this command with its default setting.
  
  Default: 45

- **max_fragments**
  
  Specifies the maximum number of IPv4/IPv6 fragments per fragment chain.

  `max_fragments` must be an integer from 1 through 300.

**Usage Guidelines**

Use this command to limit the maximum number of IPv4/IPv6 fragments.

**Examples**

The following command limits the maximum number of IPv4/IPv6 fragments to 100:

```
ip max-fragments 100
```
**label content-id**

This command allows you to specify a label (text string) to associate with a content ID for UDRs/EDRs/eG-CDRs.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

**Syntax Description**

- **label content-id** content_id text label_text
- **no label content-id** content_id

**no**

If previously configured, deletes the specified label.

**content-id content_id**

Specifies the content ID to associate with the label.  
**content_id** must be an integer from 1 through 65535.

**text label_text**

Specifies the label to associate with the specified content ID.  
**label_text** must be an alphanumeric string of 1 through 64 characters.

**Usage Guidelines**

Use this command to create a text label to associate with a content ID.  
A maximum of 2048 labels can be configured in the active charging service.

**Examples**

The following command creates the label test_charge1 to be associated with the content ID 1378:

```
label content-id 1378 text test_charge1
```
**nat allocation-failure**

This command allows you to configure the action to take when NAT IP/Port allocation fails.

---
**Important**

This command is available only in StarOS 8.3 and later releases.

---

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

*active-charging service service_name*

Entering the above command sequence results in the following prompt:

[local] *host_name*(config-acsc)#

**Syntax Description**

`nat allocation-failure send-icmp-dest-unreachable`

`{ default | no } nat allocation-failure`

**default**

Configures this command with its default setting.

Default: Packets are dropped silently

**no**

If previously enabled, disables the NAT Allocation Failure configuration. Packets are dropped silently.

**Usage Guidelines**

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.

**Examples**

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

This command allows you to configure the action to take on packets when NAT IP/NPU allocation is in progress.

---

**Important**

This command is available only in StarOS 8.3 and later releases.

---

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

**active-charging service** service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

**Syntax Description**

nat allocation-in-progress { buffer | drop }

default nat allocation-in-progress

default

Configures this command with its default setting.

Default: **buffer**

**buffer | drop**

Specifies the action to take on packets when NAT IP/NPU allocation is in progress:

- **buffer**: Buffers the packets.
- **drop**: Drops the packets.

**Usage Guidelines**

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.
The following command specifies to buffer packets when NAT IP/NPU allocation is in progress:

```
nat allocation-in-progress buffer
```
**nat ip downlink reassembly-timeout**

This command configures the downlink IP reassembly timer.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

active-charging service *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**
```
[ default ] nat ip downlink reassembly-timeout *timeout*
```

*default*

Configures this command with its default setting.
Default: 2000 milliseconds

*timeout*

The maximum duration for which IP packet fragments can be retained, in milliseconds.
*timeout* must be an integer from 1 through 30000.

**Usage Guidelines**
Use this command to configure the downlink IP reassembly timer by setting the duration for which IP packet fragments can be retained.

**Examples**
The following command configures the duration for IP packet fragments with a timeout setting of 3000 seconds:
```
nat ip downlink reassembly-timeout 3000
```
nat tcp-2msl-timeout

This command allows you to configure the TCP 2MSL (Maximum Segment Lifetime) timeout value for NAT.

**Important**

This command is available only in StarOS 8.3 and later releases.

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acrs) #
```

**Syntax Description**

```
nat tcp-2msl-timeout timeout
default nat tcp-2msl-timeout
```

**default**

Configures this command with its default setting.

Default: 60 seconds

**timeout**

Specifies the TCP 2MSL timeout period, in seconds.

`timeout` must be an integer from 30 through 240.

**Usage Guidelines**

Use this command to configure the TCP 2MSL timeout value for NAT.

**Examples**

The following command configures the TCP 2MSL timeout for NAT to 120 seconds:

```
nat tcp-2msl-timeout 120
```
nat unsolicited-pkts

This command allows you to configure unsolicited packets.

**Product**

ACS  
NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

```plaintext
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```plaintext
[local]host_name(config-acs)#
```

**Syntax Description**

```plaintext
nat unsolicited-pkts { icmp-host-unreachable { max-rate packets_num } | server-list { max-limit servers_num } }  
| default | no | nat unsolicited-pkts { icmp-host-unreachable | server-list }
```

**default**

Configures this command with its default setting.

Default: Disabled

**no**

Configures this command with its default setting.

**icmp-host-unreachable max-rate packets_max**

Configures the maximum number of allowed ICMP response packets, in seconds.

*packets_max* must be an integer from 1 through 100.

**server-list max-limit servers_num**

Configures the maximum number of servers to be stored per Session Manager instance.

*servers_num* must be an integer from 2 through 50.

**Usage Guidelines**

Use the following command to configure the number of allowed ICMP responses per second to 10:

```plaintext
The following command configures a maximum of 50 unsolicited packets.
```
nat unsolicited-pkts host-unreachable max-rate 10
The following command configures the number of servers to be stored as 20:

nat unsolicited-pkts server-list max-limit 20
p2p-ads-group

This command configures the P2P Advertisement server and associated protocols/applications.

**Product**
ADC

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**

```
[ no ] p2p-ads-group ads_group_name [ -noconfirm ]
```

- **no**
  If previously configured, disables the configured correlation group.

- **ads_group_name**
  Specifies the name of the P2P Advertisement correlation group. *ads_group_name* must be an alphanumeric string of 1 through 63 characters.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**

Use this command to configure the P2P Advertisement server and associated protocols/applications.

---

**Important**

The maximum number of advertisement groups that can be configured is 100.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-acs-p2p-ads)#
```

Also see the *P2P Advertisement Server Group Configuration Mode Commands* chapter.
Examples

The following command specifies to configure the ad-server correlation group named `group1`:

```
p2p-ads-group group1
```
**p2p-detection attribute**

This command enables or disables the detection of SSL renegotiation flows.

**Product**
ADC

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

**Syntax**: active-charging service *service_name*

Entering the above command sequence results in the following prompt:

[local] *host_name*(config-acs)#

**Syntax Description**

```
| no | p2p-detection attribute { attribute_list | sub_attribute_name sub_attribute_value ] }
```

**no**
If previously enabled, disables detection of SSL renegotiation flows.

**attribute_list**
List of configurable P2P detection attributes populated from the currently loaded P2P plugin.
Supported attribute: **ssl-renegotiation**

**sub_attribute_name**
List of configurable P2P detection sub-attributes related to the attribute selected from the attribute list. This list is populated from the currently loaded P2P plugin.
Supported sub-attributes if selected attribute is **ssl-renegotiation**:

- **max-entry-per-sessmgr**: Specifies maximum SSL Session IDs tracked per session manager.
- **id-reduce-factor**: Specifies by how much factor the SSL ID is stored in the SSL Session ID tracker table. Possible values are 1, 2, 4.

**sub_attribute_value**
Value of the selected sub-attribute. If sub-attribute is not specified, the default value set in the P2P plugin will be used.

The value for **max-entry-per-sessmgr** must be an integer from 1 through 65535. Default: 20000
Possible values for `id-reduce-factor` are 1,2,4. Default: 4

**Usage Guidelines**  Use this command to enable or disable the detection of SSL renegotiation flows.

**Examples**  The following command enables SSL renegotiation with SSL session IDs as 40000 and factor as 4:

```
p2p-detection attribute ssl-renegotiation max-entry-per-sessmgr 40000 id-reduce-factor 4
```
p2p-detection behavioral

This command enables or disables behavioral detection for unidentified traffic.

**Product**
ADC

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**
```
[ no ] p2p-detection behavioral { behavioral_list | all }
```

- **no**
  If previously configured, disables the behavioral configuration.

- **behavioral_list**
  Specifies the behavior to match. The behavioral list is the list of supported behavioral detection logic populated from the currently loaded ADC plugin.

  `behavioral_list` must be one of the following:

  - **all**: Enables all behavioral detection types supported by the ADC plugin
  - **download**: Detects unknown flows which are data download using behavioral analysis
  - **p2p**: Detects P2P and file sharing protocols using behavioral analysis
  - **upload**: Detects unknown flows which are data upload using behavioral analysis
  - **video**: Detects video flows using behavioral analysis
  - **voip**: Detects VoIP (voice and video) protocols using behavioral analysis

**Usage Guidelines**
Use this command to enable or disable behavioral detection for unidentified traffic. Behavioral VoIP is meant for zero day detection of VoIP traffic. Behavioral upload/download is similar to client-server upload/download using HTTP, FTP, SFTP, etc. It must also detect flows of non-standard ports which ECS cannot detect and falls under the client-server model. The behavioral feature is disabled by default.
Examples

The following command specifies to configure behavioral VoIP:

```
p2p-detection behavioral voip
```
**p2p-detection ecs-analysis**

This command enables or disables ECS analysis for analyzers — FTP, HTTP, HTTPS, RTSP and SIP.

**Product**

ADC

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**

```
[ no ] p2p-detection ecs-analysis { all | ftp | http | https | rtsp | sip }
```

- **no**
  - If previously enabled, disables the configured analyzers.

- **all**
  - ECS analysis for all analyzers — FTP, HTTP, RTSP and SIP.

- **ftp**
  - ECS analysis for FTP analyzer.

- **http**
  - ECS analysis for HTTP analyzer.

- **https**
  - ECS analysis for HTTPS analyzer.

- **rtsp**
  - ECS analysis for RTSP analyzer.

- **sip**
  - ECS analysis for SIP analyzer.
Usage Guidelines

Use this command to enable or disable the interworking of analyzers — FTP, HTTP, RTSP and SIP. This feature is enabled by default if P2P protocols are enabled.

Examples

The following command enables ECS analysis for the ftp analyzer:

```
p2p-detection ecs-analysis ftp
```
**p2p-detection protocol**

This command enables/disables the detection of all or specified peer-to-peer (P2P) protocols.

**Product**
ADC

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

**active-charging service service_name**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**

```
[no] p2p-detection protocol [8tracks|actionvoip|actsync|adobeconnect|aimini|all|amazoncloud
|amazonmusic|amazonvideo|antsp2p|apple-push|apple-store|applejuice|applemaps|ares
|armagettron|avi|badoo|baidumovie|battlefield|bbm|beatport|bitcasa|bittorrent|bittorrent-sync
|blackberry-store|blackberry|blackdialer|box|callofduty|chikka|cisco-jabber|citrix|clubpenguin
|clubbox|comodounite|crackle|crossfire|cyberghost|ddlink|didi|directconnect|dish-anywhere
|dofus|dropbox|ebuddy|edonkey|espn|facebook|facetime|fandor|fasttrack|feidian|fical
|fiesta|filetopia|flash|flickr|floresnia|foursquare|fox-sports|freenet|friendster|fring|funshion
|gadegadu|gamekit|gmail|gnutella|go90|goober|google-music|google-push|google|googleplay
|googleplus|gotomeeting|gtalk|guildwars|halflife2|hamachivpn|hbo|hbonow|hettell|htg
|hike-messenger|hls|hotspotvpn|hulu|hyves|iax|icall|icecast|icloud|idrive|igo|iheartradio
|imesh|imessage|ingur|imo|implus|instagram|iplayer|iptv|irc|isakmp|isocket|itunes|jabber
|jap|jumilo|kakaotalk|kim-messenger|kontiki|kugoo|kuo|linkedln|lync|magicjack|manolito
|maphfactor|mapi|maplestory|meboo|megep|mig33|mlb|mojo|monkey3|mozy|msn|mstrp
|mute|mypeople|myspace|nateontalk|naverline|navigon|nbc-sports|netflix|netmotion|newsy
|nimbus|nokia-store|octoshape|off|ogg|oist|ooovoo|opendrive|openvpn|opera
|oscar|outlook|paltalk|pando|path|pcanywhere|periseo|pinterest|plingm|poco
|popo|pplive|ppstream|ps3|qq|qqgame|qqlive|quake|quic|quicktime|radio-paradise|rdp
|rdt|regram|rfactor|rhapy|rmstream|rod|rynga|samsung-store|scydo|secondlife|shoutcast
|showtime|silverlight|siri|skinny|skydrive|skype|slacker-radio|slingbox|slingtv|smartvoip
|snapchat|softether|sopcast|soribada|soulmeet|soundcloud|spdy|speedtest|splashfire|spotify
|ssdp|ssl|starz|stealthnet|steam|stun|sudiphone|svplayer|tagged|talkatone|tango|teamspeak
|teamviewer|telegram|thunder|tmo-tv|tor|truecaller|truephone|tube|tunelnradio|tunnelvoice
|tvants|tvplayer|twitter|twitter|ultrabac|ultrasonic|univision|upc-phone|usenet|ustream
|uusee|vchat|veoh|vessel|vevo|viber|video|vappdiscount|vopium|voxer|vpnx|vtok|vtun
|vudu|warcf3|wave|webyte|wechat|webi|whatapp|wii|windows-azure|windows-store|winmx
|winny|wmstream|wofangfu|wofwarcraft|wuala|xbloom|xdc|xing|yahoo|yahoosina|youku
|yourfree_tunnel|youtube|zattoo+]
```
no
If previously enabled, disables the detection of the specific peer-to-peer protocol.

all
Specifies to detect all supported P2P protocols.
In 12.2 and earlier releases: Specifying all is the same as configuring each of the following protocols individually.
In 14.0 and later releases: Specifying all means all of the protocols supported by the currently loaded plugin.

8tracks
Specifies to detect 8tracks protocol.

actionvoip
Specifies to detect ActionVoip protocol.

actsync
Specifies to detect ActiveSync protocol.

adobeconnect
Specifies to detect Adobe Connect protocol.

aimini
Specifies to detect Aimini protocol.

amazoncloud
Specifies to detect AmazonCloud protocol.

amazonmusic
Specifies to detect Amazon Music protocol.

amazonvideo
Specifies to detect Amazon Video protocol.

antsp2p
Specifies to detect ANts P2P protocol.

apple-push
Specifies to detect Apple Push Notification protocol.

apple-store
Specifies to detect iPhone Appstore protocol.
applejuice
Specifies to detect Applejuice protocol.

applemaps
Specifies to detect Apple Maps protocol.

ares
Specifies to detect Ares Galaxy protocol.

armagetron
Specifies to detect Armagetron protocol.

avi
Specifies to detect AVI protocol.

badoo
Specifies to detect Badoo protocol.

battlefld
Specifies to detect Battlefield protocol.

bbm
Specifies to detect BBM protocol.

bitcasa
Specifies to detect Bitcasa protocol.

bittorrent
Specifies to detect BitTorrent protocol.

bittorrent-sync
Specifies to detect BitTorrent Sync protocol.

blackberry-store
Specifies to detect Blackberry World protocol.

blackberry
Specifies to detect BlackBerry protocol.

blackdialer
Specifies to detect Blackdialer protocol.
box
Specifies to detect BOX protocol.

callofduty
Specifies to detect Call of Duty protocol.

chikka
Specifies to detect Chikka protocol.

cisco-jabber
Specifies to detect Cisco Jabber protocol.

citrix
Specifies to detect Citrix Independent Computing Architecture (ICA) protocol.

clubbox
Specifies to detect Clubbox protocol.

clubpenguin
Specifies to detect Club Penguin protocol.

comodounite
Specifies to detect Comodo EasyVPN protocol.

cyberghost
Specifies to detect CyberGhost VPN protocol.

crackle
Specifies to detect Crackle protocol.

crossfire
Specifies to detect Crossfire protocol.

ddlink
Specifies to detect DDLink protocol.

didi
Specifies to detect DiDi protocol.

directconnect
Specifies to detect Direct Connect protocol.
**dish-anywhere**
Specifies to detect Dish Anywhere protocol.

**dofus**
Specifies to detect DOFUS protocol.

**dropbox**
Specifies to detect Dropbox protocol.

**ebuddy**
Specifies to detect eBuddy protocol.

**edonkey**
Specifies to detect eDonkey protocol.

**espn**
Specifies to detect ESPN protocol.

**facebook**
Specifies to detect Facebook protocol.

**facetime**
Specifies to detect FaceTime protocol.

**fandor**
Specifies to detect Fandor protocol.

**fasttrack**
Specifies to detect FastTrack protocol.

**feidian**
Specifies to detect Feidian protocol.

**ficall**
Specifies to detect Ficall protocol.

**fiesta**
Specifies to detect FIESTA protocol.

**filetopia**
Specifies to detect Filetopia protocol.
flash
Specifies to detect Flash protocol.

flickr
Specifies to detect Flickr protocol.

florensia
Specifies to detect Florensia protocol.

foursquare
Specifies to detect Foursquare protocol.

fox-sports
Specifies to detect Fox Sports protocol.

freenet
Specifies to detect Freenet protocol.

friendster
Specifies to detect Friendster protocol.

fring
Specifies to detect Fring SIP protocol.

funshion
Specifies to detect Funshion protocol.

gadugadu
Specifies to detect Gadu-Gadu protocol.

gamekit
Specifies to detect GameKit protocol.

gmail
Specifies to detect Gmail protocol.

gnutella
Specifies to detect Gnutella protocol.

go90
Specifies to detect Go90 protocol.
**goober**  
Specifies to detect Goober protocol.

**google-music**  
Specifies to detect Google Music protocol.

**google-push**  
Specifies to detect Google Push Notification protocol.

**google**  
Specifies to detect Google protocol.

**googleplay**  
Specifies to detect GooglePlay protocol.

**googleplus**  
Specifies to detect GooglePlus protocol.

**gotomeeting**  
Specifies to detect Gotomeeting protocol.

**gtalk**  
Specifies to detect Google Talk protocol.

**guildwars**  
Specifies to detect GuildWars protocol.

**halflife2**  
Specifies to detect Half-Life 2 protocol.

**hamachivpn**  
Specifies to detect Hamachi VPN protocol.

**hbogo**  
Specifies to detect HBO Go protocol.

**hbonow**  
Specifies to detect HBO NOW protocol.

**heytell**  
Specifies to detect HeyTell protocol.
hgtv
Specifies to detect HGTV protocol.

hike-messenger
Specifies to detect Hike Messenger protocol.

hls
Specifies to detect HLS protocol.

hotspotvpn
Specifies to detect HotSpot VPN protocol.

hulu
Specifies to detect Hulu protocol.

hyves
Specifies to detect Hyves protocol.

iax
Specifies to detect Inter-Asterisk eXchange protocol.

icall
Specifies to detect iCall protocol.

icecast
Specifies to detect Icecast protocol.

icloud
Specifies to detect iCloud protocol.

idrive
Specifies to detect iDrive protocol.

igo
Specifies to detect IGO protocol.

iheartradio
Specifies to detect iHeartRadio protocol.

imesh
Specifies to detect iMesh protocol.
imessage
Specifies to detect iMessage protocol.

imgur
Specifies to detect Imgur protocol.

imo
Specifies to detect Imo.im instant messenger protocol.

implus
Specifies to detect IM+ protocol.

instagram
Specifies to detect Instagram protocol.

iplayer
Specifies to detect BBC iPlayer protocol.

iptv
Specifies to detect IPTV protocol.

irc
Specifies to detect Internet Relay Chat protocol.

isakmp
Specifies to detect Internet Security Association and Key Management Protocol.

iskoot
Specifies to detect iSkoot VoIP protocol.

itunes
Specifies to detect iTunes protocol.

jabber
Specifies to detect Jabber XMPP protocol.

jumbo
Specifies to detect Jumbo protocol.

jap
Specifies to detect Jap protocol.
kakaotalk
Specifies to detect Kakao Talk protocol.

kik-messenger
Specifies to detect Kik Messenger protocol.

kontiki
Specifies to detect Kontiki delivery protocol.

kugoo
Specifies to detect Kugoo protocol.

kuro
Specifies to detect Kuro protocol.

linkedin
Specifies to detect Linkedin protocol.

lync
Specifies to detect Microsoft Lync protocol.

magicjack
Specifies to detect MagicJack protocol.

manolito
Specifies to detect MANOLITO protocol.

mapfactor

mapi
Specifies to detect MAPI protocol.

maplestory
Specifies to detect MapleStory protocol.

meebo
Specifies to detect Meebo protocol.

mgcp
Specifies to detect Media Gateway Control Protocol.
mig33
Specifies to detect Mig33 protocol.

mlb
Specifies to detect MLB protocol.

mojo
Specifies to detect Mojo protocol.

monkey3
Specifies to detect Monkey3 protocol.

mozy
Specifies to detect Mozy protocol.

msn
Specifies to detect MSN Messenger protocol.

msrp
Specifies to detect MSRP protocol.

mute
Specifies to detect MUTE protocol.

mypeople
Specifies to detect My People protocol.

myspace
Specifies to detect MySpace protocol.

nateontalk
Specifies to detect NateOn Talk protocol.

naverline
Specifies to detect Naver Line protocol.

navigon
Specifies to detect Navigon protocol.

nbc-sports
Specifies to detect NBC Sports protocol.
netflix
Specifies to detect Netflix protocol.

netmotion
Specifies to detect NetMotion Internet Mobility Protocol.

newsy
Specifies to detect Newsy protocol.

nimbuzz
Specifies to detect Nimbuzz protocol.

nokia-store
Specifies to detect Nokia Ovi Store protocol.

octoshape
Specifies to detect Octoshape protocol.

off
Specifies to detect Off-The-Record protocol.

ogg
Specifies to detect Ogg multimedia streaming protocol.

oist
Specifies to detect Oist protocol.

ooVoo
Specifies to detect ooVoo protocol.

opendrive
Specifies to detect Opendrive protocol.

openft
Specifies to detect OpenFT protocol.

openvpn
Specifies to detect OpenVPN protocol.

operamini
Specifies to detect Operamini protocol.
orb
Specifies to detect Internet Inter-ORB Protocol.

oscar
Specifies to detect Open System for CommunicAtion in Realtime protocol.

outlook
Specifies to detect Outlook protocol.

paltalk
Specifies to detect Paltalk protocol.

pando
Specifies to detect Pando protocol.

pandora
Specifies to detect Pandora protocol.

path
Specifies to detect Path protocol.

pcanywhere
Specifies to detect PCAnywhere protocol.

periscope
Specifies to detect Periscope protocol.

pinterest
Specifies to detect Pinterest protocol.

plingm
Specifies to detect Plingm protocol.

poco
Specifies to detect Poco protocol.

popo
Specifies to detect Popo protocol.

pplive
Specifies to detect PPlive protocol.
**ppstream**
Specifies to detect PPstream protocol.

**ps3**
Specifies to detect PS3 protocol.

**qq**
Specifies to detect Tencent QQ instant messaging protocol.

**qqgame**
Specifies to detect QQgame protocol.

**qqlive**
Specifies to detect QQlive protocol.

**quake**
Specifies to detect Quake network protocol.

**quic**
Specifies to detect QUIC protocol.

**quicktime**
Specifies to detect QuickTime protocol.

**radio-paradise**
Specifies to detect Radio Paradise protocol.

**rdp**
Specifies to detect Remote Desktop protocol.

**rdt**
Specifies to detect Real Data Transport (RDT) protocol.

**regram**
Specifies to detect Regram protocol.

**rfactor**
Specifies to detect rFactor protocol.

**rhapsody**
Specifies to detect Rhapsody protocol.
**rmstream**
Specifies to detect RealMedia streaming protocol.

**rodi**
Specifies to detect Rodi protocol.

**rynga**
Specifies to detect Rynga protocol.

**samsung-store**
Specifies to detect Samsung App Store protocol.

**scydo**
Specifies to detect Scydo VoIP protocol.

**secondlife**
Specifies to detect Second Life protocol.

**shoutcast**
Specifies to detect SHOUTcast protocol.

**showtime**
Specifies to detect Showtime protocol.

**silverlight**
Specifies to detect Silverlight protocol.

**siri**
Specifies to detect Apple Siri protocol.

**skiny**
Specifies to detect Skinny Call Control Protocol (SCCP).

**skydrive**
Specifies to detect Skydrive protocol.

**skype**
Specifies to detect Skype protocol.

**slacker-radio**
Specifies to detect Slacker Radio protocol.
slingbox
Specifies to detect Slingbox protocol.

slingtv
Specifies to detect Slingtv protocol.

smartvoip
Specifies to detect SmartVoip protocol.

snapchat
Specifies to detect SnapChat protocol.

softether
Specifies to detect Softether protocol.

sopcast
Specifies to detect Sopcast streaming protocol.

soribada
Specifies to detect Soribada protocol.

soulseek
Specifies to detect Soulseek chat and file transfer protocol.

spdy
Specifies to detect SPDY protocol.

speedtest
Specifies to detect Speedtest protocol.

splashfighter
Specifies to detect SplashFighter protocol.

spotify
Specifies to detect Spotify music streaming protocol.

ssdp
Specifies to detect Simple Service Discovery Protocol.

ssl
Specifies to detect SSL Protocol.
starz
Specifies to detect Starz Play protocol.

stealthnet
Specifies to detect StealthNet RShare network protocol.

steam
Specifies to detect Steam file transfer protocol.

stun
Specifies to detect Session Traversal Utilities for NAT protocol.

sudaphone
Specifies to detect Sudaphone protocol.

svtplay
Specifies to detect SVTPlay protocol.

tagged
Specifies to detect Tagged protocol.

talkatone
Specifies to detect Talkatone protocol.

tango
Specifies to detect TAco Next Generation Objects hardware control system protocol.

teamspeak
Specifies to detect TeamSpeak VoIP gaming client protocol.

teamviewer
Specifies to detect TeamViewer remote control protocol.

telegram
Specifies to detect Telegram protocol.

thunder
Specifies to detect Thunder (Xunlei) download manager protocol.

tmo-tv
Specifies to detect TMO TV protocol.
tor
Specifies to detect Tor hidden service (anonymizer) protocol.

truecaller
Specifies to detect Truecaller protocol.

truphone
Specifies to detect Truphone WiFi VoIP protocol.

tumblr
Specifies to detect Tumblr protocol.

tunein-radio
Specifies to detect TuneIn Radio protocol.

tunnelvoice
Specifies to detect Tunnel VoIP protocol.

tvants
Specifies to detect TVAnts protocol.

tvuplayer
Specifies to detect TVUPlayer protocol.

twitch
Specifies to detect Twitch protocol.

twitter
Specifies to detect Twitter protocol.

ultrabac
Specifies to detect UltraBac protocol.

ultrasurf
Specifies to detect UltraSurf protocol.

univision
Specifies to detect Univision Deportes protocol.

upc-phone
Specifies to detect UPC Phone protocol.
**usenet**
Specifies to detect Usenet Network News Transfer Protocol (NNTP) protocol.

**ustream**
Specifies to detect Ustream protocol.

**uusee**
Specifies to detect UUSee on-demand streaming protocol.

**vchat**
Specifies to detect VChat protocol.

**veohtv**
Specifies to detect VeohTV television via Internet protocol.

**vessel**
Specifies to detect Vessel protocol.

**vevo**
Specifies to detect Vevo protocol.

**viber**
Specifies to detect Viber VoIP protocol.

**vine**
Specifies to detect Vine protocol.

**voipdiscount**
Specifies to detect VoipDiscount protocol.

**vopium**
 Specifies to detect Vopium protocol.

**voxer**
Specifies to detect Voxer Walkie Talkie protocol.

**vpnx**
Specifies to detect VPN-X cross-platform protocol.

**vtok**
Specifies to detect Vtok protocol.
vtun
Specifies to detect VTun (Virtual Tunnel) protocol.

vudu
Specifies to detect Vudu protocol.

warcft3
Specifies to detect Warcraft 3 game protocol.

waze
Specifies to detect Waze protocol.

webex
Specifies to detect Webex protocol.

wechat
Specifies to detect Wechat protocol.

weibo
Specifies to detect Weibo protocol.

whatsapp
Specifies to detect WhatsApp messaging protocol.

wii
Specifies to detect Wii Remote Bluetooth protocol.

windows-azure
Specifies to detect Windows Azure Cloud Services protocol.

windows-store
Specifies to detect Windows Phone App Store protocol.

winmx
Specifies to detect WinMX Peer Network Protocol (WPNP).

winny
Specifies to detect Winny anonymizing protocol.

wmstream
Specifies to detect Windows Media HTTP Streaming Protocol.
wofkungfu
Specifies to detect wofkungfu protocol.

wofwarcraft
Specifies to detect World of Warcraft gaming protocol.

wuala
Specifies to detect Wuala protocol.

xbox
Specifies to detect Xbox protocol.

xdcc
Specifies to detect eXtended Direct Client-to-Client protocol.

xing
Specifies to detect Xing protocol.

yahoo
Specifies to detect Yahoo! Messenger protocol.

yahoomail
Specifies to detect Yahoo Mail protocol.

youku
Specifies to detect Youku protocol.

yourfreetunnel
Specifies to detect yourfree Tunnel chat protocol.

youtube
Specifies to detect Youtube protocol.

zattoo
Specifies to detect Zattoo IPTV protocol.

+
More than one of the above keywords can be entered within a single command.

Usage Guidelines
Use this command to configure the detection of all or specific P2P protocol(s). Multiple keywords can be specified in a single command.
**Examples**

The following command enables detection of all P2P protocols:

```
p2p-detection protocol all
```
packet-filter

This command allows you to create/configure/delete ACS packet filters.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs)#

**Syntax Description**
packet-filter packet_filter_name [ -noconfirm ]
no packet-filter packet_filter_name

no
If previously configured, deletes the specified packet filter from the active charging service.

packet_filter_name
Specifies the packet filter to add/configure/delete.

packet_filter_name must be the name of a packet filter, and must be an alphanumeric string of 1 through 63 characters. Each packet filter must have a unique name.

If the named packet filter does not exist, it is created, and the CLI mode changes to the ACS Packet Filter Configuration Mode wherein the packet filter can be configured.

If the named packet filter already exists, the CLI mode changes to the ACS Packet Filter Configuration Mode for that packet filter.

-noconfirm
Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**
Use this command to create/configure/delete an ACS packet filter.

On entering this command, the CLI prompt changes to:

[context_name]hostname(config-packet-filter)#
Also see the *ACS Packet Filter Configuration Mode Commands* chapter.

**Examples**

The following command creates a packet filter named *filter3*, and enters the ACS Packet Filter Configuration Mode:

```
packet-filter filter3
```
**passive-mode**

This command allows you to configure the Active Charging Service to operate in passive mode, wherein ACS passively monitors copies of packets.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**

```
[ default | no ] passive-mode
```

- **no**
  If previously enabled, disables the passive mode configuration.

- **default**
  Configures this command with its default setting.
  Default: Disabled

**Usage Guidelines**
Use this command to put the active charging service in/out of passive mode operation, wherein ACS passively monitors copies of packets.

**Examples**
The following command puts the active charging service into passive mode operation:

```
passive-mode
```
pcp-service

Creates or deletes a Port Control Protocol (PCP) service.

Important
This command is customer specific. Contact your Cisco account representative for more information.

Product
ACS
NAT
PSF

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax Description
| no | pcp-service pcp_service_name | -noconfirm |

no
If previously configured, deletes the specified PCP service.

pcp_service_name
Specifies the name of a PCP service.

pcp_service_name must be the name of a PCP service, and must be an alphanumeric string of 1 through 63 characters. A maximum of 5 PCP services can be configured in the active charging service.

If the named PCP service does not exist, it is created, and the CLI mode changes to the PCP Configuration Mode wherein the service can be configured. If the named PCP service already exists, the CLI mode changes to the PCP Configuration Mode.

-noconfirm
Specifies that the command must execute without any additional prompt and confirmation from the user.
Usage Guidelines

Use this command to create or delete a PCP service.

On entering this command, the CLI prompt changes to:

[context_name]hostname(config-pcp-service)#

Also see the PCP Configuration Mode Commands chapter.

Examples

The following command creates a PCP service named `pcp1`, and changes to the PCP Configuration mode:

```
pcp-service pcp1
```
policy-control bearer-bw-limit

This command allows you to enable/disable per-bearer MBR policing—bandwidth limiting.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

**Syntax Description**
{ default | no } policy-control bearer-bw-limit

default
Configures this command with its default setting.
Default: Enable; by default, per-bearer MBR policing is enabled.

no
Disables per-bearer MBR policing.

**Usage Guidelines**
This command allows you to enable/disable per-bearer bandwidth limiting based on bitrates received over Gx. Note that there are only two variants of this command, the default and no variants.
policy-control bind-default-bearer

For PCEF Bearer Binding in 3G and when BCM mode is UE only, this command allows you to enable/disable binding rules having QoS of default bearer to the default bearer and to not ignore/ignore other rules.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

```text
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
``` 

**Syntax Description**
| default | no | policy-control bind-default-bearer |

```text
default
```

Configures this command with its default setting.

Default: Disables only binding those rules having QoS of default bearer to the default bearer and specifies to not ignore other rules. Rules having respective QoS will get attached to the relevant bearers. Also TFT updates towards the UE (access side) will not be suppressed.

```text
no
```

The no keyword functionality is same as the default setting.

**Usage Guidelines**
This CLI command is used to bind all the PCC dynamic or predef rules received from PCRF (Bearer Control Mode (BCM) is UE_only) without QoS and ARP or with the same QoS and ARP as that of the default bearer, to the default bearer. This CLI is used for UE_Only mode.

In case no QoS is specified the rule gets attached to the default bearer. Also no TFT updates will be sent towards UE (access side). So only one default bearer will ever be created.

On receiving a PCC dynamic rule or predef rule from PCRF, having QoS/ARP other than the default bearer, then those rules are ignored and a response indicating that the rule could not be installed, is sent.

This CLI command will not work currently for dedicated bearers (secondary PDP contexts). Secondary bearers initiated by UE are not supported.
Releases prior to 12.2, when UE_Only BCM is received from PCRF, IMSA terminates the call for P-GW (GnGp setup). Release 12.2 onwards, the P-GW call is not terminated so as to be in compliance with 3GPP standard specification TS 29.212, but Traffic Flow Template (TFT) updates towards UE (access side) will be supported.

**Important**

This CLI is applicable to all the rulebases in the chassis configuration. If the rulebase is changed to some other rulebase in the interim period or anytime later, this CLI will continue to apply to the current new rulebase too.
policy-control burst-size

This command allows you to configure the burst size for bandwidth limiting per dynamic-rule or per bearer.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs)#
```

**Syntax Description**
```
policy-control burst-size { auto-readjust [ duration duration ] | bytes bytes } 
{ default | no } policy-control burst-size
```

- `default | no`
  Configures this command with its default setting.
  Default: 65535 bytes

- `duration duration`
  Configures the burst size equal to <seconds> of traffic.
  `duration` must be an integer from 1 through 20.
  Default: In 12.1 and earlier releases, 10 seconds. In 12.2 and later releases, 5 seconds.

- `bytes bytes`
  Specifies the burst size, in bytes.
  `bytes` must be an integer from 1 through 4000000000.

**Usage Guidelines**
Use this command to configure the burst size for bandwidth limiting per dynamic-rule or per bearer.

**Examples**
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-action-override

This command has been removed from the ACS Configuration Mode, and replaced by the charging-action-override command in the ACS Rulebase Configuration Mode.
policy-control charging-rule-base-name

This command allows you to configure how the Charging-Rule-Base-Name AVP from PCRF is interpreted, either as ACS rulebase or ACS group-of-ruledefs.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

*active-charging service service_name*

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

**Syntax Description**

policy-control charging-rule-base-name { active-charging-group-of-ruledefs | active-charging-rulebase
[ ignore-when-removed ] [ use-first ]
default policy-control charging-rule-base-name
no policy-control charging-rule-base-name active-charging-rulebase use-first

default
Configures this command with its default setting(s).
Default:

- **charging-rule-base-name**: active-charging-group-of-ruledefs
- **use-first**: Disabled

no
If multiple Charging-Rule-Base-Name are received from the PCRF, specifies to select the last rulebase. This is the default behavior.

*active-charging-group-of-ruledefs*
Specifies interpreting Charging-Rule-Base-Name as ACS group-of-ruledefs.

*active-charging-rulebase [ ignore-when-removed ] [ use-first ]*
Specifies interpreting Charging-Rule-Base-Name as ACS rulebase.
When Charging-Rule-Base-Name AVP is interpreted as ACS 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.

**ignore-when-removed**: Specifies to ignore PCRF request for removal of Charging-Rule-Base-Name, and take no action. If this keyword is not configured, the PDP context from which the rulebase is removed gets terminated.

**use-first**: If multiple Charging-Rule-Base-Name are received from the PCRF, since a call can only have one ACS rulebase applied, specifies to select the first rulebase. If previously enabled, to disable this configuration, use the `no policy-control charging-rule-base-name active-charging-rulebase use-first` command. If this keyword is not configured, by default, the last rulebase is selected.

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 Guidelines

Use this command to configure interpretation of Charging-Rule-Base-Name AVP from PCRF either as ACS group-of-rules or as ACS rulebase.

### Examples

The following command configures interpreting of Charging-Rule-Base-Name AVP as ACS rulebase:

```
policy-control charging-rule-base-name active-charging-rulebase
```
 policy-control dynamic-rule-limit

This command allows you to enable/disable per-dynamic-rule MBR policing—bandwidth limiting.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:
```
[local]host_name(config-acs)#
```

**Syntax Description**
```
{ default | no } policy-control dynamic-rule-limit
```

- **default**
  Configures this command with its default setting.
  Default: Enable; by default, per-dynamic-rule MBR policing is enabled.

- **no**
  Disables per-dynamic-rule MBR policing.

**Usage Guidelines**
This command allows you to enable/disable per-dynamic-rule bandwidth limiting based on bitrates received over Gx. Note that there are only two variants of this command, the default and no variants.
policy-control l7-dynamic-rules

This command allows you to enable/disable the L7 capabilities through Charging-Rule-Definition AVP received over Gx interface.

Important

This CLI command is license dependant. Contact your Cisco account representative for more information on the licensing requirements.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs) #

Syntax Description

| default | no | policy-control l7-dynamic-rules |

default

Configures this command with its default setting.
Default: Disabled i.e. activation of L7 dynamic rules through Charging-Rule-Definition AVP will be disabled.

no

Disables the activation of L7 dynamic rules through Charging-Rule-Definition AVP if already activated.

Usage Guidelines

This command allows you to enable/disable the L7 capabilities through Charging-Rule-Definition AVP received over Gx interface.

In releases prior to 20, only up to L4 dynamic rule provisioning and activation was supported by the gateway.
In release 20, the dynamic rule is extended to support L7 capabilities. This is accomplished by introducing these two optional Diameter AVPs "L7-Application-Description" and "Rule-Condition-Action" as part of the grouped AVP "Charging-Rule-Definition".

When Out-of-Credit (OOC) trigger is sent from OCS to PCRF, L7 dynamic rule is sent from PCRF along with a condition and action which allow the subscriber to access specific URLs. The condition is the trigger
when to apply the action. For example: If OOC (quota exhaustion condition) is sent from OCS, PCEF should allow (action) all the packets matching that rule (rating-group) to pass through. Once the relocation of credit occurs the gateway reverts back the special treatment for these URLs.

This feature is configured in such a way that PCEF/PCRF is able to fully support L7 dynamic rules and thereby enabling dynamic routes to redirect L7 traffic.

---

**Important**

This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for more information on the licensing requirements.

For more information on this feature, refer to the *ECS Administration Guide*. 
policy-control retransmissions-counted

This command allows you to enable/disable charging of retransmitted packets when they hit a dynamic rule.

**Important**
In release 17.0, this command has been deprecated. This configuration is available at rulebase level as [local]host_name(config-rule-base)# [no] retransmissions-counted.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

**active-charging service service_name**
Entering the above command sequence results in the following prompt:
[local]host_name(config-acs)#

**Syntax Description**
| default | no | policy-control retransmissions-counted |

| default | no |
Disables charging of retransmitted packets when they hit a dynamic rule.
Default: Disabled; no retransmissions counted.

**Usage Guidelines**
Use this command to enable/disable charging of retransmitted packets when they hit a dynamic rule.

**Examples**
The following command enables retransmissions to be charged when they hit a dynamic rule:

```
policy-control retransmissions-counted
```
**policy-control update-default-bearer**

For PCEF Bearer Binding in 4G, this command allows you to enable/disable binding rules having QoS of default bearer to the default bearer and to not ignore/ignore other rules.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**

| default | no | **policy-control update-default-bearer** |

**default**

Configures this command with its default setting.

Disables only binding those rules having QoS of default bearer to the default bearer and specifies to not ignore other rules. Rules having respective QoS will get attached to the relevant bearers. Also TFT updates towards UE (access side) will not be suppressed.

**no**

Enables binding rules having QoS of default bearer to the default bearer and specifies to ignore other rules. In case no QoS is specified the rule gets attached to default bearer. Also TFT updates towards UE (access side) will be suppressed for default bearer. So only one default-bearer will ever be created.

**Caution**

Upon executing this CLI command "no policy-control update-default-bearer", system crash is likely to occur if the TFT information is not added to the charging-action.

**Usage Guidelines**

This CLI command is used to bind all the PCC dynamic or predef rules received from PCRF without QoS and ARP or with the same QoS and ARP as that of the default bearer, to the default bearer.

On receiving a PCC dynamic rule or predef rule from PCRF, having QoS/ARP other than the default bearer, then those rules are ignored and a response indicating that the rule could not be installed, is sent.
This CLI command will not work currently for dedicated bearers (secondary PDP contexts). Secondary bearers initiated by UE are not supported.

Releases prior to 12.2 TFT updates were sent towards the UE (access side) on all bearers. Release 12.2 onwards, TFT updates will be suppressed towards the UE (access side) for default bearer, if the CLI is enabled.

---

**Important**

This CLI is applicable to all the rulebases in the chassis configuration. If the rulebase is changed to some other rulebase in the interim period or anytime later, this CLI will continue to apply to the current new rulebase too.
port-map

This command allows you to create/configure/delete port maps.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs)#

Syntax Description

port-map port_map_name | -noconfirm |

no port-map port_map_name

no

If previously configured, deletes the specified port map from the active charging service.

port_map_name

Specifies the port map to add/configure/delete.

port_map_name must be the name of a port map, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each port map must have a unique name.

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 for that port map.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete an ACS 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.

Also see the *ACS Port Map Configuration Mode Commands* chapter.

Examples

The following command creates a port map named *portmap1*, and enters the ACS Port Map Configuration Mode:

```
port-map portmap1
```
**qos-group-of-ruledefs**

This command allows you to create/configure/delete a qos-group-of-ruledefs.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

```active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]\host_name(config-acs)#
```

**Syntax Description**

```
qos-group-of-ruledefs qos_group_of_ruledefs_name [ -noconfirm ] [ description description ]
no qos-group-of-ruledefs qos_group_of_ruledefs_name
```

- **no**
  If previously configured, deletes the specified qos-group-of-ruledefs from the active charging service.

  ```qos_group_of_ruledefs_name```

  Specifies the qos-group-of-ruledefs to add/configure/delete.

  ```qos_group_of_ruledefs_name```

  must be the name of a qos-group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters. Each qos-group-of-ruledefs must have a unique name.

  If the named qos-group-of-ruledefs does not exist, it is created, and the CLI mode changes to the ACS QoS-Group-Of-Ruledefs Configuration Mode wherein the group can be configured.

  If the named qos-group-of-ruledefs already exists, the CLI mode changes to the ACS QoS-Group-Of-Ruledefs Configuration Mode for that group.

- **-noconfirm**

  Specifies that the command must execute without prompting for confirmation.

- **description description**

  Specifies an optional description of the group, such as purpose of setting up the group, to be included in the configuration.
**Usage Guidelines**  Use this command to create/configure/delete a qos-group-of-ruledefs.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-qos-group-of-ruledefs)#
```

Also see the ACS QoS-Group-of-Ruledefs Configuration Mode Commands chapter.

**Examples**  The following command creates a qos-group-of-ruledefs named *group1*, and enters the ACS QoS-Group-of-Ruledefs Configuration Mode:

```
qos-group-of-ruledefs group1
```
radio-congestion

This command allows you to create/configure/delete Radio Congestion policy.

Important

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product

MVG

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs) #

Syntax Description

radio-congestion policy policy_name | -noconfirm |

no radio-congestion policy policy_name

no

If previously configured, deletes the specified Radio Congestion policy from the active charging service.

policy_name

Specifies the Radio Congestion policy to add/configure/delete.

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

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/configure/delete a Radio Congestion policy.

On entering this command, the CLI prompt changes to:

[context_name]hostname(config-radio-congestion-policy) #

Also see the Radio Congestion Policy Configuration Mode Commands chapter.
Examples

The following command creates a policy named `test123`, and changes to the Radio Congestion Policy Configuration Mode:

```
radio-congestion policy test123
```
readdress-server-list

This command allows you to create/delete server list for DNS redirection.

Important

This command is license dependent. For more information please contact your Cisco account representative.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax Description

| no | readdress-server-list server_list_name | -noconfirm |

no

If previously configured, deletes the specified readdress server list from the active charging service.

server_list_name

Specifies the server list to add/configure/delete for DNS redirection.

server_list_name must be an alphanumeric string of 1 through 63 characters and can contain punctuation characters. Each server list must have a unique name.

If the named server list does not exist, it is created, and the CLI mode changes to the ACS Readdress Server List Configuration Mode wherein the servers can be configured.

If the named server list already exists, the CLI mode changes to the ACS Readdress Server List Configuration Mode for that server list.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create/delete server list for DNS redirection.
To add the servers to the server list, see the `server` command in the *ACS Readdress Server List Configuration Mode* chapter.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-readdress-server-list)#
```

Also see the *ACS Readdress Server List Configuration Mode* chapter.

### Examples

The following command creates a charging action named `homeDNSserver` and changes to the ACS Readdress Server List Configuration Mode:

```
readdress-server-list homeDNSserver
```
redirect user-agent

This command allows you to specify the user agent for conditional redirection of traffic flows.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax Description**

```
| no | redirect user-agent user_agent_name
```

- **no**
  If previously configured, deletes the specified user agent from the active charging service.

  **user_agent_name**
  Specifies the user agent to be used for redirecting traffic flow.

  - **user_agent_name** must be the name of a user agent, and must be an alphanumeric string of 1 through 32 characters.
  - A maximum of 16 user-agents can be configured in the active charging service.

**Usage Guidelines**

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 ACS Charging Action Configuration Mode.

**Examples**

The following command specifies the redirect user agent `user_rule1` for conditional redirection of traffic flow:

```
redirect user-agent user_rule1
```
rulebase

This command allows you to create/configure/delete ACS rulebases.

Important

A maximum of 512 rulebases can be configured in the active charging service.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

(host_name) (config-acs)#

Syntax Description

rulebase rulebase_name [ -noconfirm ]

no rulebase rulebase_name

- no

If previously configured, deletes the specified rulebase from the active charging service.

rulebase_name

Specifies the rulebase to add/configure/delete.

rulebase_name must be the name of an ACS rulebase, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each rulebase must have a unique name.

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 for that rulebase.

- noconfirm

Specifies that the command must execute without prompting for confirmation.
Usage Guidelines

Use this command to create/configure/delete an ACS rulebase. A rulebase is a collection of protocol rules to match a flow and associated actions to be taken for matching flow.

The default rulebase is used when a subscriber/APN is not configured with a specific rulebase to use.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-rule-base)#
```

Also see the ACS Rulebase Configuration Mode Commands chapter.

Examples

The following command creates a rulebase named `test1`, and enters the ACS Rulebase Configuration Mode:

```
rulebase test1
```
rulebase-list

This command allows you to create and delete ACS rulebase lists.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax Description

rulebase-list rulebase_list_name rulebase_name [ rulebase_name + ]

no rulebase-list rulebase_list_name

no

If previously configured, deletes the specified rulebase list from the active charging service.

rulebase_list_name

Specifies the rulebase list to add/modify/delete.

rulebase_list_name must be the name of an ACS rulebase list, and must be an alphanumeric string of 1 through 63 characters.

rulebase_name

Specifies the rulebase name(s) to add to the rulebase list.

Each rulebase list must contain a minimum of one rulebase name, and the cumulative length of all rulebase names must not exceed 256 bytes.

rulebase_name must be the name of an ACS rulebase, and each rulebase name must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to create or delete an ACS rulebase list. A rulebase list is a space-separated string of rulebase names supplied to the OCS, from which the OCS chooses the rulebase to use for the subscriber. The rulebase list to use for a subscriber is specified in the APN for the subscriber.

In 12.3 and earlier releases, a maximum of 20 rulebase lists can be configured.
In 14.0 and later releases, a maximum of 128 rulebase lists can be configured.
See the active-charging rulebase-list command in the APN Configuration Mode Commands chapter.

Examples

The following command creates a rulebase list named rblit, and adds the rulebases named rulebase1, rulebase3, and rulebase5 to it:

```
rulebase-list rblist rulebase1 rulebase3 rulebase5
```

The following command deletes the rulebase list named rblist:

```
no rulebase-list rblist
```
ruledef

This command allows you to create/configure/delete ACS rule definitions.

Important

A maximum of 2048 ruledefs can be configured in the active charging service.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax Description

ruledef ruledef_name [ -noconfirm ]

no ruledef ruledef_name

no

If previously configured, deletes the specified ruledef from the active charging service.

ruledef_name

Specifies the ruledef to add/configure/delete.

ruledef_name must be the name of an ACS ruledef, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each ruledef must have a unique name. 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 for that ruledef.
If there are any changes to ruledef and the Override Control/Inheritance feature is enabled, then execute the CLI command "update active-charging override-control rulebase-config". For more information on this command, see the Command Line Interface Reference.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

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.

On entering this command, the CLI prompt changes to:

[context_name]hostname(config-acs-ruledef)#

Also see the ACS Ruledef Configuration Mode Commands chapter.

Examples

The following command creates an ACS ruledef named test1, and enters the ACS Ruledef Configuration Mode:

ruledef test1
service-scheme

This command allows you to enable association of service-scheme based on trigger events.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax Description | no | service-scheme service_scheme_name | -noconfirm |

no
If previously configured, deletes the specified service scheme configuration from the active charging service.

service_scheme_name
Specifies the service scheme to add/configure/delete.

service_scheme_name must be a service scheme name, and must be an alphanumeric string of 1 through 63 characters.

-noconfirm
Specifies that the command must execute without prompting for confirmation.

Usage Guidelines Use this command to create/configure/delete a service-scheme and enable association of service-scheme based on trigger events.

On entering this command, the CLI prompt changes to:

[context_name]hostname(config-acs-servscheme)#

Also see the ACS Service Scheme Configuration Mode Commands chapter.
Examples

The following command creates a service scheme named ss1 and changes to the ACS Service Scheme Configuration Mode:

```
service-scheme ss1
```
sip advanced

This command enables SIP ALG to maintain the same tag parameters (from and to tag) for Authorization or Proxy Authentication requests.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

**active-charging service service_name**

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs)#
```

**Syntax Description**
`| default | no | sip advanced out-of-dialog-request retain-tag`

**default**
Configures this command with its default setting.
Default: Disabled

**no**
If previously enabled, disables the SIP ALG configuration.

**Usage Guidelines**
Use this command to enable SIP ALG to maintain the same tag parameters (from and to tag) while processing 4xx responses for Authorization or Proxy Authentication requests as described in section 8.1.3.5 of RFC 3261 (SIP: Session Initiation Protocol).
statistics-collection

This command allows to dynamically enable collection of Charging, Firewall or Post-processing ruledef statistics.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs)#

Syntax Description
statistics-collection { all | ruledef { all | charging | firewall | post-processing } } { default | no } statistics-collection

default
Configures this command with its default setting. By default, statistics collection is disabled.

no
Disables dynamic statistics collection.

all
Specifies to collect all statistics.

ruledef
Specifies to collect ruledef statistics.

all | charging | firewall | post-processing

• all: Specifies to collect all ruledef statistics.
• charging: Specifies to collect charging ruledef statistics.
• firewall: Specifies to collect firewall ruledef statistics.
• post-processing: Specifies to collect post-processing ruledef statistics.
Usage Guidelines

Use this command to dynamically enable collection of ruledef statistics — Charging, Firewall or Post-processing. By default, the statistics will not be maintained. If the command is not configured, statistics collection will not be enabled and the following error message will be displayed in the `show active-charging sessions full` CLI — "statistics collection disabled; not collecting <charging/firewall/postprocessing> ruledef stats".

Example

The following command will collect firewall ruledef statistics:

`statistics-collection ruledef firewall`
**subs-class**

This command allows you to configure Active Charging Service subscriber class.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs)#
```

**Syntax Description**

```
[ no | subs-class subs_class_name [ -noconfirm ]
```

- **no**
  If previously configured, deletes the specified configuration from the active charging service.

- **subs_class_name**
  Specifies the subscriber class to add/configure/delete.
  `subs_class_name` must be an alphanumeric string of 1 through 63 characters.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**

Use this command to create/configure/delete a subscriber class.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-acs-subclass)#
```

Also see the *ACS Subscriber Class Configuration Mode Commands* chapter.

**Examples**

The following command creates a subscriber class named `sc1` and changes to the ACS Subscriber Class Configuration Mode:

```
subs-class sc1
```
subscriber-base

This command allows you to configure Active Charging Service subscriber base.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration

```plaintext
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```plaintext
[local]host_name(config-acs)#
```

**Syntax Description**  
| no | subscriber-base subs_base_name | -noconfirm |

- **no**  
  If previously configured, deletes the specified configuration from the active charging service.

- **subs_base_name**  
  Specifies the subscriber base to add/configure/delete.  
  `subs_base_name` must be an alphanumeric string of 1 through 63 characters.

- **-noconfirm**  
  Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**  
Use this command to create/configure/delete a subscriber base. Only one subscriber-base configuration is currently allowed and it is recommended to use the subscriber base name as `default`.  

On entering this command, the CLI prompt changes to:

```plaintext
[context_name]hostname(config-subscriber-base)#
```

Also see the *ACS Subscriber Base Configuration Mode Commands* chapter.

**Examples**  
The following command creates a subscriber base named `default` and changes to the ACS Subscriber Base Configuration Mode:

```plaintext
subscriber-base default
```
system-limit l4-flows

This command allows you to configure the system-wide Layer 4 flow limit.

Important
This command is customer specific. For more information contact your Cisco account representative.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs) #

Syntax Description
system-limit l4-flows limit
{ default | no } system-limit l4-flows

default
Configures this command with its default setting.
Default: Disabled; same as no system-limit l4-flows

no
Disables the limit checking configuration.

limit
Specifies the Layer 4 flows limit.
limit must be an integer from 1 through 2147483647.

Usage Guidelines

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 the 5-tuple key. If the "Effective Flows" exceeds the "System-wide Flow Limit", the Resource Manager indicates it to the active charging service. When ACS 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 active charging service a change in behavior is indicated to active charging 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.

Examples

The following command sets the system limit for L4 flows to 100:

```
  system-limit l4-flows 100
```
tethering-database

This command allows you to enable/disable the Tethering Detection feature, and load the databases from the specified files into the service.

**Important**

This command is available only if the **Smartphone Tethering Detection** license is enabled. Contact your Cisco account representative for more information.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

**active-charging service** service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

**Syntax Description**

```
tethering-database [ ipv6-os-signature ipv6os_signature_db_file_name | os-signature os_signature_db_file_name | tac tac_db_file_name | ua-signature ua_signature_db_file_name ] +
{ default | no } tethering-database
```

- **default**
  Configures this command with its default setting.
  Default: Tethering Detection feature is disabled, and the database file names are reset to their default values.

- **no**
  Disables Tethering Detection.

- **ipv6-os-signature ipv6os_signature_db_file_name**
  Specifies the IPv6 OS Signature database file to load.
  *ipv6os_signature_db_file_name* must be the name of the IPv6 OS Signature database file, and must be an alphanumeric string of 1 through 255 characters.
  Default filename: *v6-os-db*
**os-signature os_signature_db_file_name**
Specifies the OS Signature database file to load.

*os_signature_db_file_name* must be the name of the OS Signature database file, and must be an alphanumeric string of 1 through 255 characters.

Default filename: *os-db*

**tac tac_db_file_name**
Specifies the TAC database file to load.

*tac_db_file_name* must be the name of a TAC database file, and must be an alphanumeric string of 1 through 255 characters.

Default filename: *tac-db*

**ua-signature ua_signature_db_file_name**
Specifies the User Agent (UA) Signature database file to load.

*ua_signature_db_file_name* must be the name of a UA Signature database file, and must be an alphanumeric string of 1 through 255 characters.

Default filename: *ua-db*

```
+
```
Indicates that more than one of the preceding option can be entered in a single command.

**Usage Guidelines**

Use this command to enable the Tethering Detection feature, and load the OS, TAC, and UA databases from the specified files into the service.

Tethering refers to the use of a smartphone as a USB dongle/modem to provide Internet connectivity to laptops/PDAs/tablets like iPad, using the smartphone's data plan. Typically many operators have in place an eat-all-you-can-get data plan for smartphones, the usage of which is intended to be from the smartphone as a mobile device. However, some users use the low rate/unlimited usage of data plan to provide Internet connectivity to their laptops in places where normal Internet connection via broadband/WiFi might be more costly/not available/insecure.

Operators are interested in detecting such usage of a smartphone as a modem to better understand the usage across their networks and offer plans inline to that usage to their customers. They may also charge the tethered and non-tethered traffic separately.

After Tethering Detection has been enabled here (regardless, it must also be enabled within the rulebase), this CLI command may be used to change the databases with the specified databases.

The files are picked from the disk file system within the /databases directory. If a file name value is not configured, the default file names, *v6-os-db*, *os-db*, *tac-db*, and *ua-db*, are used.

For more information on the Tethering Detection feature, refer to the *Enhanced Charging Services Administration Guide*.

**Examples**

The following command enables Tethering Detection and selects the UA Signature database file named *test*:

```
tethering-database ua-signature test
```
tethering-detection

This command allows you to enable tethering detection for TAC-db lookup and bypass tethering detection based on Interface ID.

Product: ACS

Privilege: Security Administrator, Administrator

Command Modes: Exec > ACS Configuration

Syntax Description:

```
[no] tethering-detection { bypass interface-id ifid | tac-db }
```

- **no**
  If previously configured, disables the specified configuration for tethering detection.

- **bypass interface-id ifid**
  Specifies the IPv6 Interface ID from IPv6 address. When configured, all IPv6 flows having this interface ID in the source IP address will bypass IP-TTL and OS based tethering detection.
  By default, tethering detection bypass will be disabled.
  *ifid* is a 64-bit unsigned integer from IPv6 address.

- **tac-db**
  Enables TAC-db lookup for tethering detection. This is the default behavior.

Usage Guidelines

Use this command to enable TAC-db lookup for tethering detection or bypass tethering detection based on Interface ID.

For more information on the Tethering Detection feature, refer to the Enhanced Charging Services Administration Guide.

Examples

The following command enables TAC-db lookup for tethering detection:

```
tethering-detection tac-db
```


**timedef**

This command allows you to create/configure/delete ACS Time Definitions (timedefs).

---

**Important**

This command is available only in StarOS 8.1 and in StarOS 9.0 and later releases.

---

**Important**

A maximum of 10 timedefs can be configured in the active charging service.

---

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

active-chargingservice service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)\

**Syntax Description**

timedef timedef_name [ -noconfirm ]

no timedef timedef_name

- **no**
  - If previously configured, deletes the specified timedef from the active charging service.

- **timedef_name**
  - Specifies the timedef to add/configure/delete.

  *timedef_name* must be the name of a timedef, and must be an alphanumeric string of 1 through 63 characters. Each timedef must have a unique name.

  If the named timedef does not exist, it is created, and the CLI mode changes to the ACS Timedef Configuration Mode wherein timeslots for the timedef can be configured.

  If the named timedef already exists, the CLI mode changes to the ACS Timedef Configuration Mode for that timedef.
-noconfirm
Specifies that the command must execute without prompting for confirmation.

Usage Guidelines
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.

On entering this command, the CLI prompt changes to:

[context_name]hostname(config-acs-timedef)#

Also see the ACS Timedef Configuration Mode Commands chapter.

Examples
The following command creates a timedef named test1, and enters the ACS Timedef Configuration Mode:

timedef test1
tpo policy

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
tpo profile

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
trigger-action

This command allows you to configure ACS trigger actions.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax Description

| no | trigger-action trigger_action_name | -noconfirm |

no
If previously configured, deletes the specified trigger action from the active charging service.

trigger_action_name
Specifies the trigger action to add/configure/delete.

trigger_action_name must be the name of a trigger action, and must be an alphanumeric string of 1 through 63 characters.

If the named trigger action does not exist, it is created, and the CLI mode changes to the ACS Trigger Action Configuration Mode.

-noconfirm
Specifies that the command must execute without prompting for confirmation.

Usage Guidelines
Use this command to create/configure/delete an ACS trigger action.

On entering this command, the CLI prompt changes to:

[context_name]hostname(config-acs-trig-action)#

Also see the ACS Trigger Action Configuration Mode Commands chapter.
Examples

The following command creates a trigger action named *ta1* and changes to the ACS Trigger Action Configuration Mode:

```
trigger-action ta1
```
**trigger-condition**

This command allows you to configure ACS trigger conditions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs)#
```

**Syntax Description**

```
| no |trigger-condition trigger_condn_name | -noconfirm |
```

- **no**
  If previously configured, deletes the specified trigger condition from the active charging service.

- **trigger_condn_name**
  Specifies the trigger condition to add/configure/delete.
  `trigger_condn_name` must be an alphanumeric string of 1 through 63 characters.
  If the named trigger condition does not exist, it is created, and the CLI mode changes to the ACS Trigger Condition Configuration Mode.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**

Use this command to create/configure/delete an ACS trigger condition.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-acs-trig-condn)#
```

Also see the *ACS Trigger Condition Configuration Mode Commands* chapter.
Examples

The following command creates a trigger condition named \textit{tc1} and changes to the ACS Trigger Condition Configuration Mode:

\texttt{trigger-condition tc1}
udr-format

This command allows you to create/configure/delete a User Data Record (UDR) format.

A maximum of 256 UDR plus EDR formats can be configured in the active charging service.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration
active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]\(host\_name\)(config-acs)#

Syntax Description
udr-format udr_format_name | -noconfirm |
no udr-format udr_format_name

- no
If previously configured, deletes the specified UDR format from the active charging service.

udr_format_name
Specifies the UDR format to add/configure/delete.

udr_format_name must be the name of a UDR format, and must be an alphanumeric string of 1 through 63 characters. Each UDR format must have a unique name.

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 for that UDR format.

- noconfirm
Specifies that the command must execute without prompting for confirmation.

Usage Guidelines
Use this command to create/configure/delete a UDR format in the active charging service.
On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-acs-udr)#
```

Also see the *UDR Format Configuration Mode Commands* chapter.

**Examples**

The following command creates an UDR format named *udr_format1* and changes to the UDR Format Configuration Mode:

```
udr-format udr_format1
```
url-blacklisting match-method

This command allows you to specify the match method to look up URLs in the URL Blacklisting database.

**Product**

CF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration

*active-charging service service_name*

Entering the above command sequence results in the following prompt:

[local]\host_name(config-acs)#

**Syntax Description**

url-blacklisting match-method { exact | generic }
default url-blacklisting match-method

default

Configures this command with its default setting.

Default: exact

---

**In 14.0 and later releases, it is recommended to use the generic match method for URL Blacklisting.**

**exact**

Specifies the exact-match method, wherein URL Blacklisting is performed only on exact match with a URL present in the URL Blacklisting database.

**generic**

Specifies the generic-match method, wherein URL Blacklisting is performed on a generic match with URLs present in the URL Blacklisting database.

**Usage Guidelines**

Use this command to set the match method to look up URLs in the URL Blacklisting database.
Examples

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 allows you to create/configure/delete ACS extension-header (x-header) format specifications.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration

*active-charging service service_name*

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

**Syntax Description**

- `xheader-format xheader_format_name` | `-noconfirm` |
- `no xheader-format xheader_format_name`

- **no**
If previously configured, deletes the specified x-header format from the active charging service.

  **xheader_format_name**
Specifies the x-header format to add/configure/delete.

  *xheader_format_name* must be the name of an xheader format, and must be an alphanumeric string of 1 through 63 characters. Each x-header format must have a unique name.

  If the named x-header format does not exist, it is created, and the CLI mode changes to the ACS 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 ACS X-header Format Configuration Mode for that x-header format.

  **-noconfirm**
Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**
Use this command to create/configure/delete an x-header format specification in the active charging service.

On entering this command, the CLI prompt changes to:

[context_name]hostname(config-acs-xheader)#
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 *ACS Charging Action Configuration Mode Commands* chapter. Also see the *ACS X-header Format Configuration Mode Commands* chapter.

**Examples**

The following command creates an x-header format named *test*, and enters the ACS X-header Format Configuration Mode:

```
xheader-format test
```
ACS Group-of-Objects Configuration Mode Commands

The ACS Group-of-Objects Configuration Mode is used to configure groups of Active Charging Service (ACS) objects.

Important
This configuration mode is available only in 10.2 and later releases.

Command Modes
Exec > ACS Configuration > ACS Group-of-Objects Configuration

active-charging service service_name > group-of-objects object_name [ type string ]

Entering the above command sequence results in the following prompt:

[local]{host_name}{config-acs-group-of-objects}#

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

- end, page 544
- exit, page 545
- member-object, page 546
**end**

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

**Usage Guidelines**
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 Description
exit

Usage Guidelines
Use this command to return to the parent configuration mode.
**member-object**

This command allows you to add or remove objects from the current group-of-objects.

---

**Important**

A maximum of 128 objects can be added to a group-of-objects.

---

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > ACS Group-of-Objects Configuration

```
active-charging service service_name > group-of-objects object_name [ type string ]
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-group-of-objects)#
```

**Syntax Description**

```
[ no ] member-object object
```

- **no**
  
  If previously added, removes the specified member object from the current group-of-objects.

- **object**
  
  Specifies the member object to add to or remove from the current group-of-objects. 
  
  **object** must be an alpha and/or numeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to add or remove member objects from a group-of-objects.

**Examples**

The following command adds the object *test* to the current group-of-objects:

```
member-object test
```
ACS Group-of-Prefixed-URLs Configuration Mode

**Commands**

This configuration mode is customer specific. For more information, contact your Cisco account representative.

The ACS Group-of-Prefixed-URLs Configuration Mode is used to create and configure groups of prefixed URLs.

**Command Modes**

Exec > ACS Configuration > ACS Group-of-Prefixed-URLs Configuration

`active-charging service service_name > group-of-prefixed-urls group_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-grp-of-prefixed-urls)#
```

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

- end, page 548
- exit, page 549
- prefixed-url, page 550
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

der end

Usage Guidelines

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 Description**
exit

**Usage Guidelines**
Use this command to return to the parent configuration mode.
prefixed-url

This command allows you to add or remove URLs from the current group of prefixed URLs.

Important
A maximum of 10 URLs can be added per group.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > ACS Group-of-Prefixed-URLs Configuration

active-charging service service_name > group-of-prefixed-urls group_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-grp-of-prefixed-urls)#

Syntax Description
[ no ] prefixed-url url

no
If added previously, removes the specified URL from the current group of prefixed URLs.

url
Specifies the URL to add/remove.
url must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines
Use this command to add or remove URLs to be filtered from the group of prefixed URLs.

Examples
The following command adds the URL http://abc.net to the current group of prefixed URLs:
prefixed-url http://abc.net
ACS Group-of-Ruledefs Configuration Mode Commands

The ACS Group-of-Ruledefs Configuration Mode is used to configure groups of rule definitions (ruledefs).

Important
In 14.1 and earlier releases, a maximum of 64 group-of-ruledefs can be configured. In 15.0 and later releases, a maximum of 128 group-of-ruledefs can be configured.

Command Modes
Exec > ACS Configuration > ACS Group-of-Ruledefs Configuration

active-charging service service_name > group-of-ruledefs group_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-group-of-ruledefs)#

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

- add-ruledef, page 552
- dynamic-command, page 554
- end, page 555
- exit, page 556
- group-of-ruledefs-application, page 557
add-ruledef

This command allows you to add or remove ruledefs from a group-of-ruledefs.

### Important

A maximum of 128 ruledefs can be added to a group-of-ruledefs.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > ACS Group-of-Ruledefs Configuration

active-charging service service_name > group-of-ruledefs group_name

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-group-of-ruledefs)#
```

**Syntax Description**

add-ruledef priority ruledef_priority ruledef ruledef_name

no add-ruledef priority ruledef_priority

no

If previously configured, specifies that the ruledef associated with the specified priority number be removed from the current group-of-ruledefs.

**priority ruledef_priority**

Specifies priority of the ruledef in the current group-of-ruledefs. **ruledef_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 an ACS ruledef, and must be an alpha and/or numeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to add/remove ruledefs from a group-of-ruledefs.
A group-of-ruledefs can 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.

Examples

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
```
dynamic-command

This command allows you to add or remove dynamic commands from a group-of-ruledefs.

**Product**
ACS
CF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > ACS Group-of-Ruledefs Configuration
`active-charging service service_name > group-of-ruledefs group_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-group-of-ruledefs)#
```

**Syntax Description**

- `dynamic-command content-filtering category policy-id policy_id`
- `no dynamic-command content-filtering category policy-id`

`no`
Specifies to remove dynamic command configuration from the current group-of-ruledefs.

`content-filtering category policy-id policy_id`
Specifies the dynamic command for Content Filtering Category Policy ID configuration. `policy_id` must be a Content Filtering Category Policy ID, and must be an integer from 1 through 4294967295.

**Usage Guidelines**
Use this command to add a dynamic command to a group-of-ruledefs, which will be executed when a dynamic protocol specifies that group-of-ruledefs (via the Rulebase-Name AVP).

- **Important**
  This release supports only one command option, which is `dynamic-command content-filtering category policy-id policy_id`

**Examples**
The following command configures a dynamic command for Content Filtering Category Policy ID configuration using the policy ID 100:

```
dynamic-command content-filtering category policy-id 100
```
end

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

Product       All

Privilege      Security Administrator, Administrator

Syntax Description  end

Usage Guidelines  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 Description

exit

Usage Guidelines

Use this command to return to the parent configuration mode.
**group-of-ruledefs-application**

This command allows you to specify the purpose of setting up a group-of-ruledefs as either charging, post-processing, or for other purposes.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > ACS Group-of-Ruledefs Configuration

`active-charging service service_name > group-of-ruledefs group_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-group-of-ruledefs)#
```

**Syntax Description**

```
group-of-ruledefs-application { charging | content-filtering | gx-alias | post-processing | tpo }
no group-of-ruledefs-application
```

- **no**
  
  If previously configured, deletes the group-of-ruledefs-application configuration from the current group-of-ruledefs.

- **charging**
  
  Specifies that the current group-of-ruledefs is for charging purposes.

- **content-filtering**
  
  Specifies that the current group-of-ruledefs is for content-filtering purposes.

- **gx-alias**
  
  Specifies that the current group-of-ruledefs is for Gx-alias purposes.

- **post-processing**
  
  Specifies that the current group-of-ruledefs is for post-processing purposes, that is, for use by the **post-processing** CLI command or automatic name-matching to the Diameter Filter-Id AVPs.
The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

**Usage Guidelines**

Use this command to specify the purpose of setting up a group-of-ruledefs. If not specified, by default the rule-application type will be charging.

If the group-of-ruledefs-application is configured for content-filtering, no ruledef can be added to it. Similarly, if configured explicitly for charging or post-processing, a content-filtering policy cannot be configured in it.

The group-of-ruledefs may be dynamically selected by Diameter, as described by the **policy-control charging-rulebase-name** command in the Active Charging Service Configuration Mode. If so selected, the priority field of the add-ruledef instances within the group-of-ruledefs are ignored, and all of the rules named by the ruledef keyword that are also configured with the same name in the **action** command are selected.

**Examples**

The following command configures the current group-of-ruledefs as for post-processing purposes:

```
group-of-ruledefs-application post-processing
```
**ACS Host Pool Configuration Mode Commands**

The ACS Host Pool Configuration Mode is used to define a pool of host addresses within the ACS Configuration Mode. The host pool facilitates to create rules to handle the packets coming from or going to a group of hosts within an access policy.

**Command Modes**

Exec > ACS Configuration > ACS Host Pool Configuration

```
active-charging service service_name > host-pool host_pool_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-host-pool)#
```

**Important**

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

- end, page 560
- exit, page 561
- ip, page 562
**end**

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

end

**Usage Guidelines**

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 Description**
exit

**Usage Guidelines**
Use this command to return to the parent configuration mode.
This command allows you to add/remove an individual or a range of host IPv4/IPv6 address(es) from the current host pool.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > ACS Host Pool Configuration

`active-charging service service_name > host-pool host_pool_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-host-pool)#
```

**Syntax Description**

```
| no | ip { ipv4/ipv6_address | ipv4/ipv6_address/maskbit | range start_ipv4/ipv6_address to end_ipv4/ipv6_address }
```

- **no**
  
  If added previously, removes the specified IPv4/IPv6 address(es) from the current host pool.

- **ipv4/ipv6_address**
  
  Specifies an IPv4/IPv6 address to add to the current host pool.
  
  `ipv4/ipv6_address` must be an IPv4/IPv6 address.

- **ipv4/ipv6_address/maskbit**
  
  Specifies an IPv4/IPv6 address/mask bits combination to add to the current host pool.
  
  `ipv4/ipv6_address` must be an IPv4/IPv6 address.
  
  `maskbit` must be the number of bits in the subnet mask, and must be a numeric value.

- **range start_ipv4/ipv6_address to end_ipv4/ipv6_address**
  
  Specifies a range of IPv4/IPv6 addresses to add to the current host pool.
  
  `start_ipv4/ipv6_address` specifies the starting IPv4/IPv6 address of the range, and must be less than `end_ipv4/ipv6_address`.
  
  `end_ipv4/ipv6_address` specifies the ending IPv4/IPv6 address of the range, and must be greater than `start_ipv4/ipv6_address`. 
Usage Guidelines

Use this command to add an individual or a range of IPv4/IPv6 addresses to a host pool. Up to 10 sets of IPv4/IPv6 addresses can be configured in each host pool.

Examples

The following command adds all IPv4 addresses from 10.2.3.4 through 10.4.5.6 to the current host pool:

```
ip range 10.2.3.4 to 10.4.5.6
```
ACS IMSI Pool Configuration Mode Commands

The ACS IMSI Pool Configuration Mode is used to define a pool of subscriber International Mobile Station Identifier (IMSI) 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.

**Command Modes**

Exec > ACS Configuration > ACS IMSI Pool Configuration

```plaintext
active-charging service service_name > imsi-pool imsi_pool_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-imsi-pool)#
```

**Important**

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

- end, page 566
- exit, page 567
- imsi, page 568
**end**

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

end

**Usage Guidelines**

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 Description

exit

Usage Guidelines

Use this command to return to the parent configuration mode.
This command allows you to add/remove an individual or a range of subscriber IMSI numbers from the current IMSI pool.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > ACS IMSI Pool Configuration
active-charging service service_name > imsi-pool imsi_pool_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-imsi-pool)#

Syntax Description
| no | imsi { imsi_number | range start_imsi to end_imsi }

no
If added previously, removes the specified subscriber IMSI number(s) from the current IMSI pool.

imsi_number
Specifies an IMSI number to add to the current IMSI pool.
imsi_number must be an IMSI number, and must be a sequence of hexadecimal digits between 1 and 15.

start_imsi to end_imsi
Specifies a range of IMSI numbers to add to the current IMSI pool.
start_imsi specifies the starting IMSI number of the range and must be less than end_imsi.
end_imsi specifies the ending IMSI number of the range and must be greater than start_imsi.

Usage Guidelines
Use this command to add an individual or range of subscriber IMSI numbers to an IMSI pool. Up to 10 sets of IMSI numbers can be configured in each IMSI pool.

Examples
The following command adds IMSI numbers from 31015098765321 to 31015098765679 to the current IMSI pool:
imsi range 31015098765321 to 31015098765679
ACS Packet Filter Configuration Mode Commands

The ACS Packet Filter Configuration Mode is used to create and configure Active Charging Service (ACS) packet filters.

**Command Modes**

Exec > ACS Configuration > Packet Filter Configuration

```
active-charging service service_name > packet-filter packet_filter_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-packet-filter) #
```

**Important**

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

- direction, page 570
- end, page 571
- exit, page 572
- ip local-port, page 573
- ip protocol, page 574
- ip remote-address, page 576
- ip remote-port, page 578
- priority, page 579
direction

This command allows you to specify the direction in which the current packet filter will be applied.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Packet Filter Configuration

active-charging service service_name > packet-filter packet_filter_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-packet-filter)#

Syntax Description

direction { bi-directional | downlink | uplink }
default direction

default

Configures this command with its default setting.
Default: bi-directional

bi-directional

Specifies that the packet filter has to be applied in both uplink and downlink directions.

downlink

Specifies that the packet filter has to be applied only in the downlink direction.

uplink

Specifies that the packet filter has to be applied only in the uplink direction.

Usage Guidelines

Use this command to specify the direction in which the packet filter has to be applied.

Examples

The following command specifies that the packet filter must be applied in the downlink direction:

direction downlink
end

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

end

**Usage Guidelines**

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 Description

exit

Usage Guidelines

Use this command to return to the parent configuration mode.
ip local-port

This command allows you to configure the IP 5-tuple local port(s) for the current packet filter.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Packet Filter Configuration

```plaintext
active-charging service service_name > packet-filter packet_filter_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-packet-filter)#
```

**Syntax Description**
```plaintext
ip local-port { = port_number | range start_port_number to end_port_number }
no ip local-port
```

- **no**
  If previously configured, deletes the ip local-port configuration from the current packet filter.

- **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**
  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 Guidelines**
Use this command to configure the IP local port(s) for a packet filter.

**Examples**
The following command configures the IP local port as 456:

```plaintext
ip local-port 456
```
ip protocol

This command allows you to configure the IP protocol(s) for the current packet filter.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Packet Filter Configuration

active-charging service service_name > packet-filter packet_filter_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-packet-filter)#

Syntax Description
In StarOS 9.0 and later releases:

ip protocol = protocol_number
no ip protocol

In StarOS 8.2 and earlier releases:

ip protocol { = protocol_number | range start_protocol_number to end_protocol_number }
no ip protocol

no

If previously configured, deletes the IP protocol configuration from the current packet filter.

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

Important
In StarOS 9.0 and later releases this option is deprecated.

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.
Usage Guidelines

Use this command to configure the protocol(s) for a packet filter.

Examples

The following command configures the protocol assignment number 300:

```
ip protocol = 300
```
ip remote-address

This command allows you to configure the IP remote address(es) for the current packet filter.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Packet Filter Configuration

```
active-charging service service_name > packet-filter packet_filter_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-packet-filter)#
```

**Syntax Description**

In StarOS 9.0 and later releases:

```
ip remote-address = { ipv4/ipv6_address | ipv4/ipv6_address/mask }
no ip remote-address
```

In StarOS 8.2 and earlier releases:

```
ip remote-address { = { ipv4/ipv6_address | ipv4/ipv6_address/mask } | range { start_ipv4/ipv6_address | start_ipv4/ipv6_address/mask } to { end_ipv4/ipv6_address | end_ipv4/ipv6_address/mask } } }
no ip remote-address
```

```
no
```

If previously configured, deletes the IP remote-address configuration from the current packet filter.

```
ip remote-address = { ipv4/ipv6_address | ipv4/ipv6_address/mask }
```

- `<ipv4/ipv6_address>` specifies the IPv4/IPv6 address.
- `<ipv4/ipv6_address/mask>` specifies the IPv4/IPv6 address and the number of subnet bits representing the subnet mask in shorthand.

```
ip remote-address range { start_ipv4/ipv6_address | start_ipv4/ipv6_address/mask } to { end_ipv4/ipv6_address | end_ipv4/ipv6_address/mask }
```

**Important**

In StarOS 9.0 and later releases this keyword has been deprecated.

**range** specifies a range of IPv4/IPv6 addresses.
**Usage Guidelines**

Use this command to configure the remote address(es) for a packet filter.

**Examples**

The following command configures the IP remote address as 10.2.3.4/24:

```bash
ip remote-address = 10.2.3.4/24
```
**ip remote-port**

This command allows you to configure the IP remote port(s) for the current packet filter.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Packet Filter Configuration

active-charging service service_name > packet-filter packet_filter_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-packet-filter)#

**Syntax Description**

```
ip remote-port { = port_number | range start_port_number to end_port_number }  
no ip remote-port
```

**no**

If previously configured, deletes the ip remote-port configuration from the current packet filter.

**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**

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 Guidelines**
Use this command to configure the IP remote port(s) for a packet filter.

**Examples**
The following command configures the IP remote port as 789:

`ip remote-port = 789`
priority

This command allows you to configure the current packet filter's priority.

---

**Important**

This command is deprecated in certain 9.0 releases and in 10.0 and later releases. The precedence values of packet filters (those from both dynamic and predefined rules) are assigned by the PCEF based on an internal process.

---

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Packet Filter Configuration

```
active-charging service service_name > packet-filter packet_filter_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-packet-filter)#
```

**Syntax Description**

```
priority priority
no priority
```

- **no**
  - If previously configured, deletes the priority configuration in the current packet filter.

  **priority**
  - Specifies this packet filter's priority
  - `priority` must be an integer from 0 through 255.

**Usage Guidelines**

Use this command to configure the packet filter's priority. The priority must be configured for the packet filter to be used in a TFT. Packets are compared against packet filters in a prioritized fashion, with 0 being the highest priority. Without this setting, this filter will not be used.

**Examples**

The following command configures the packet filter's priority as 3:

```
priority 3
```
priority
ACS Port Map Configuration Mode Commands

The ACS Port Map Configuration Mode is used to define an application-port mapping in the ACS Configuration Mode. The application-port map associates a range of TCP/UDP ports to a specific application/protocol within a rule definition (ruledef).

**Command Modes**

```plaintext
Exec > ACS Configuration > ACS Port Map Configuration

active-charging service service_name > port-map port_map_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-port-map)#
```

**Important**

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

- end, page 582
- exit, page 583
- port, page 584
**end**

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

**Usage Guidelines**
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 Description**
exit

**Usage Guidelines**
Use this command to return to the parent configuration mode.
port

Add or removes an individual or a range of TCP/UDP port numbers associated with an application or protocol from the current port map.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > ACS Port Map Configuration

active-charging service service_name > port-map port_map_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-port-map) #

Syntax Description

| no | port { port_number | range start_port_number to end_port_number }

- **no**
  - If added previously, removes the specified TCP/UDP port numbers from the current port map.

- **port_number**
  - Specifies a TCP/UDP port number to add to the current port map.
  - `port_number` is expressed as an integer from 1 through 65535.

- **range start_port_number to end_port_number**
  - Specifies a range of port numbers to add to the current port map.
  - `start_port_number` specifies the starting port number of the range, it must be an integer from 1 through 65535, and must be less than `end_port_number`.
  - `end_port_number` specifies the ending port number of the range, it must be an integer from 1 through 65535, and must be greater than `start_port_number`.

Usage Guidelines

Use this command to add an individual or a range of TCP/UDP port numbers to a port map. Up to 10 sets of ports can be configured in each port map.

Examples

The following command adds all TCP/UDP port numbers from 3112 through 5000 to the port map:

```
port range 3112 to 5000
```
ACS QoS-Group-of-Ruledefs Configuration Mode Commands

The ACS QoS-Group-of-Ruledefs Configuration Mode is used to configure groups of rule definitions (ruledefs).

Command Modes

Exec > ACS Configuration > QoS-Group-of-Ruledefs Configuration

active-charging service service_name > qos-group-of-ruledefs group_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-qos-group-of-ruledefs) #

Important

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

- add-group-of-ruledef, page 586
- add-ruledef, page 587
- end, page 588
- exit, page 589
add-group-of-ruledef

This command allows you to add or remove groups-of-ruledefs from a qos-group-of-ruledefs.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > QoS-Group-of-Ruledefs Configuration

active-charging service service_name > qos-group-of-ruledefs group_name

Entering the above command sequence results in the following prompt:

[local]\host_name(config-qos-group-of-ruledefs)#

Syntax Description

| no | add-group-of-ruledef group_of_ruledef_name

no

If added previously, removes the specified group-of-ruledef from the current qos-group-of-ruledefs.

group_of_ruledef_name

Specifies name of the group-of-ruledef to add/remove from the current qos-group-of-ruledefs.

group_of_ruledef_name must be the name of an ACS group-of-ruledef, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to add/remove a group-of-ruledefs from a qos-group-of-ruledefs.

Examples

The following command adds the group-of-ruledef named grpruledef1 to the current qos-group-of-ruledefs:

add-group-of-ruledef grpruledef1
add-ruledef

This command allows you to add or remove rule defs from a qos-group-of-rule defs.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > QoS-Group-of-Rule defs Configuration

```plaintext
active-charging service service_name > qos-group-of-rule defs group_name
```

Entering the above command sequence results in the following prompt:

[local]host_name(config-qos-group-of-rule defs)#

**Syntax Description**

```
[ no ] add-ruledef ruledef_name
```

- **no**
  If added previously, removes the specified ruledef from the current qos-group-of-rule defs.

- **ruledef_name**
  Specifies name of the ruledef to add/remove from the current qos-group-of-rule defs.
  `ruledef_name` must be the name of an ACS ruledef, and must be an alpha and/or numeric string of 1 through 63 characters.

**Usage Guidelines**
Use this command to add/remove rule defs from a qos-group-of-rule defs.

**Examples**
The following command adds the rule def `ruledef23` to the current qos-group-of-rule defs:

`add-ruledef ruledef23`
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

test

Usage Guidelines

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 Description**

exit

**Usage Guidelines**

Use this command to return to the parent configuration mode.
ACS Readdress Server List Configuration Mode

The ACS Readdress Server List Configuration Mode is used to add, configure, and delete servers to the server list for DNS redirection.

**Command Modes**

```
Exec > ACS Configuration > Readdress Server List Configuration
```

```
active-charging service service_name > readdress-server-list server_list_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-readdress-server-list)#
```

**Important**

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

- consecutive-failures, page 592
- end, page 594
- exit, page 595
- reactivation-time, page 596
- response-timeout, page 598
- server, page 600
**consecutive-failures**

This command allows you to configure the consecutive number of times a server can be unreachable after which the system marks the server as inactive.

---

**Important**

This command is license dependent. For more information contact your Cisco account representative.

---

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Readdress Server List Configuration

```bash
active-charging service service_name > readdress-server-list server_list_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-readdress-server-list)#
```

**Syntax Description**

- `consecutive-failures consecutive_failures`
- `default consecutive-failures`

- **default**
  Configures this command with its default setting.
  Default: 5

- **consecutive_failures**
  Specifies the consecutive number of times a server can be unreachable after which the system marks the server as inactive.
  `consecutive_failures` must be an integer from 1 through 10.

---

**Important**

If not explicitly configured, the default value of 5 will be used.

---

**Usage Guidelines**

Use this command to configure the consecutive number of response failures, after which a server is marked as inactive.
Examples

The following command configures the number of consecutive server response failures to 4:

```
consecutive-failures 4
```
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

**Usage Guidelines**
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 Description**

`exit`

**Usage Guidelines**

Use this command to return to the parent configuration mode.
reactivation-time

This command allows you to configure the time duration (in seconds) after which the status of a previously inactive server is rechecked.

**Important**

This command is license dependent. For more information contact your Cisco account representative.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Readdress Server List Configuration

```
active-charging service service_name > readdress-server-list server_list_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-readdress-server-list)#
```

**Syntax Description**

```
reactivation-time reactivation_time
default reactivation-time
```

- **default**
  
  Configures this command with its default setting.
  
  Default: 300 seconds

- **reactivation_time**
  
  Specifies the time duration after which the status of the inactive server is rechecked.
  
  `reactivation_time` must be an integer from 1 through 1800.

**Important**

If not explicitly configured, the default value of 300 seconds will be used.

**Usage Guidelines**

Use this command to configure the time duration (in seconds) after which the status of a previously inactive server is rechecked.
**Examples**

The following command configures the reactivation time to 180 seconds:

```
reactivation-time 180
```
response-timeout

This command allows you to configure the time duration for which the system will wait for a response from the server before marking it unreachable.

**Important**

This command is license dependent. For more information contact your Cisco account representative.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Readdress Server List Configuration

`active-charging service service_name > readdress-server-list server_list_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-readdress-server-list)#
```

**Syntax Description**

- `response-timeout`

**default response-timeout**

- `default`

Configures this command with its default setting.

Default: 1000 milliseconds

- `response_timeout`

Specifies the time duration (in milliseconds) for which the system will wait for a response from the server before marking it unreachable.

`response_timeout` must be an integer from 1 through 10000.

**Important**

If not explicitly configured, the default value of 1000 milliseconds will be used.

**Usage Guidelines**

Use this command to configure the time duration (in milliseconds) for which the system will wait for a response from the server before marking it unreachable.
Examples

The following command sets the server response timeout to 4500 milliseconds:

response-timeout 4500
This command allows you to configure the DNS server(s) to which flow will be readdressed.

**Important**
This command is license dependent. Contact your Cisco account representative for more information.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Readdress Server List Configuration

```
active-charging service service_name > readdress-server-list server_list_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-readdress-server-list) #
```

**Syntax Description**

```
server [ ipv4_address | ipv6_address ] [ port port_number ]
no server [ ipv4_address ]
```

**no**
If previously configured, disables the specified server configuration.

```
ipv4_address | ipv6_address
```
Specifies the IP address of the DNS server.

*ipv4_address* must be expressed in IPv4 dotted-decimal notation format.

*ipv6_address* must be expressed in IPv6 colon-separated-hexadecimal notation.

```
port port_number
```
Specifies the TCP port of the DNS server.

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

**Usage Guidelines**
Use this command to configure the DNS server(s) to which the flow will be readdressed based on the contents of the Fully Qualified Domain Name (FQDN).
Examples

The following commands configure the DNS servers for packet flow to 192.168.12.101, 192.168.12.102, and 2607:f0d0:1002:51::4/64:

- server 192.168.12.101
- server 192.168.12.102
- server 2607:f0d0:1002:51::4/64

The following command removes the DNS server configuration for 192.168.12.101 that was configured above:

- no server 192.168.12.101
ACS Rulebase Configuration Mode Commands

The ACS Rulebase Configuration Mode is used to configure Active Charging Service (ACS) rulebases.

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

**active-charging service** service_name > **rulebase** rulebase_name

Entering the above command sequence results in the following prompt:

[local] *host_name* (config-rule-base)#

**Important**

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

- action priority, page 607
- active-charging rf, page 611
- bandwidth default-policy, page 613
- billing-records, page 614
- cca diameter requested-service-unit, page 616
- cca quota, page 618
- cca quota time-duration algorithm, page 620
- cca radius accounting interval, page 622
- cca radius charging context, page 624
- cca radius user-password, page 625
- charging-action-override, page 626
- charging-rule-optimization, page 628
- check-point accounting, page 630
- constituent-policies, page 632
• content-filtering category policy-id, page 634
• content-filtering flow-any-error, page 636
• content-filtering mode, page 637
• credit-control-group, page 639
• description, page 641
• dynamic-rule order, page 642
• edr edr-dcca-fh, page 643
• edr p2p, page 645
• edr nemo-call, page 647
• edr sn-charge-volume, page 649
• edr suppress-zero-byte-records, page 651
• edr transaction-complete, page 652
• edr voip-call-end, page 654
• egcdr inactivity-meter, page 656
• egcdr cdr-encoding, page 657
• egcdr tariff, page 659
• egcdr threshold, page 661
• egcdr time-duration algorithm, page 663
• end, page 665
• exit, page 666
• extract-host-from-uri, page 667
• firewall dos-protection, page 669
• firewall flooding, page 672
• firewall icmp-destination-unreachable-message-threshold, page 674
• firewall max-ip-packet-size, page 676
• firewall mime-flood, page 678
• firewall no-ruledef-matches, page 680
• firewall policy, page 683
• firewall priority, page 685
• firewall tcp-first-packet-non-syn, page 689
• firewall tcp-idle-timeout-action, page 690
• firewall tcp-reset-message-threshold, page 691
• firewall tcp-syn-flood-intercept, page 693
• flow any-error, page 695
• flow control-handshaking, page 697
• flow end-condition, page 699
• flow limit-across-applications, page 702
• flow rtsp-all-pkts, page 704
• fw-and-nat default-policy, page 706
• http header-parse-limit, page 708
• ip reassembly-timeout, page 710
• ip reset-tos, page 711
• nat binding-record, page 712
• nat policy, page 714
• nat suppress-aaa-update call-termination, page 716
• override-control, page 717
• p2p dynamic-flow-detection, page 720
• pcp service, page 721
• post-processing dynamic, page 722
• post-processing policy, page 724
• post-processing priority, page 726
• qos-renegotiate timeout, page 728
• radius threshold, page 729
• retransmissions-counted, page 731
• ran bandwidth optimize, page 732
• route priority, page 734
• rtp dynamic-flow-detection, page 739
• rtsp initial-bytes-limit, page 740
• ruledef-parsing, page 741
• tcp 2msl-timeout, page 743
• tcp check-window-size, page 745
• tcp mss, page 746
• tcp out-of-order-timeout, page 748
• tcp packets-out-of-order, page 749
• tcp proxy-mode, page 752
• tethering-detection, page 754
• tft-notify-ue-def-bearer, page 756
• timestamp rounding, page 757
• tpo default-policy, page 759
• transactional-rule-matching, page 760
• transport-layer-checksum, page 762
• udr threshold, page 764
• udr trigger, page 766
• url-blacklisting action, page 768
• url-preprocessing, page 770
• video optimization-preprocessing cae-readdressing, page 771
• websocket flow-detection, page 772
• wtp out-of-order-timeout, page 773
• wtp packets-out-of-order, page 774
• xheader-encryption, page 776
action priority

This command allows you to configure the action priority for a ruledef / group-of-ruledefs in the current rulebase.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**
```
action priority action_priority { [ dynamic-only | adc | mute ] | [ static-and-dynamic | timedef timedef_name ] | [ group-of-ruledefs ruledefs_group_name | ruledef ruledef_name ] charging-action charging_action_name [ monitoring-key monitoring_key ] [ description description ] }
no action priority action_priority
```

**No**
If previously configured, deletes the specified action priority configuration from the current rulebase.

**Priority action_priority**

Specifies a priority for the specified ruledef / group-of-ruledefs in the current rulebase.

*action_priority* must be unique in the current rulebase, and must be an integer from 1 through 65535.

The priority controls the order in which this instance of the CLI command will be examined. Lower numbered priorities are examined first. Up to 2048 instances may be configured, totaled among all rulebases.

**Important**

If there are any changes to action priority and the Override Control/Inheritance feature is enabled, then execute the CLI command "update active-charging override-control rulebase-config". For more information on this command, see the Command Line Interface Reference.

**Dynamic-only**

Enables matching of dynamic rules with static rules for this action priority on a flow.
Configuring the **dynamic-only** keyword 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. Default: Disabled

**adc**

Specifies the ruledef to be given as ADC rule. This keyword is optional and only visible when configured with the **dynamic-only** keyword. Default: Disabled

**mute**

Disables application reporting to PCRF. This keyword is optional and visible only after configuring the **adc** keyword. Default: Disabled

**static-and-dynamic**

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. Default: Enabled

---

**timedef** *timedef_name*

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 activate or deactivate ruledefs / group-of-ruledefs, making them available for rule matching only when they are active.

*timedef_name* must be the name of a timedef, and must be an alphanumeric string of 1 through 63 characters.

A timedef can be used with several ruledefs / group-of-ruledef. 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-ruledef, 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-ruledef is considered.

**Important** The time considered for timedef matching is the system's local time.
**ruledef ruledef_name**

Adds the specified ruledef to the current rulebase.

*ruledef_name* must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

If the specified ruledef does not exist, there will be no ruledef triggers for this action priority within the current 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 ruledefs_group_name**

Adds the specified group-of-ruledefs to the current rulebase.

*ruledefs_group_name* must be the name of a group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.

When a group-of-ruledefs is specified, if any of the ruledefs within the group matches, the specified charging-action is applied, 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 a charging action, and must be an alphanumeric string of 1 through 63 characters.

If the specified charging action does not exist, there will be no charging action triggers for this action priority within the current rulebase.

---

**Important**

If the charging action specified here is not configured or is later deleted, the system will not apply 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 alphanumeric string of 1 through 63 characters.
Usage Guidelines

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.

Examples

The following command assigns a rule and action with the action priority of 23, a ruledef named test, and a charging action named test1 to the current rulebase:

```
action priority 23 ruledef test charging-action test1
```
active-charging rf

This command allows you to enforce default rating group / service identifier on all PCC rules, predefined ACS rules, and static ACS rules for Rf-based accounting.

Important
This command is customer specific. For more information contact your Cisco account representative.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax Description

active-charging rf { rating-group-override rating_group | service-id-override service_id } { default | no } active-charging rf { rating-group-override | service-id-override }

default
Configures this command with its default setting.
Default: Override configuration is disabled; same as no.

no
Disables the override configuration.

no active-charging rf rating-group-override: Rating group override will not be enforced on the PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own rating group, it will continue to use that.

no active-charging rf service-id-override: Service ID override will not be enforced on the PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own service ID, it will continue to use that.

rating-group-override rating_group
Enforces the specified rating group on all PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own rating group, it will be overridden by the specified rating group.
rating_group must be an integer from 1 through 65535.

service-id-override service_id

Enforces the specified service ID on all PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own service ID, it will be overridden by the specified service ID.

service_id must be an integer from 1 through 65535.

Usage Guidelines

Use this command to enforce a specific rating group/service identifier on all PCC rules, predefined ACS rules, and static ACS rules for Rf-based accounting. As this CLI configuration is applied at the rulebase level, all the APNs that have the current rulebase defined will inherit the configuration.

Examples

The following command configures the service ID 100:

```
active-charging rf service-id-override 100
```
bandwidth default-policy

This command allows you to configure the default bandwidth policy for the current rulebase.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base) #
```

**Syntax Description**

- `bandwidth default-policy bandwidth_policy_name | fallback-enabled | no bandwidth default-policy`

  - `no`
    
    If previously configured, deletes the bandwidth default-policy configuration from the current rulebase.

  - `bandwidth_policy_name`
    
    Specifies the default bandwidth policy for the current rulebase.
    
    `bandwidth_policy_name` must be the name of a bandwidth policy, and must be an alphanumeric string of 1 through 63 characters.

  - `fallback-enabled`
    
    Determines whether policy under rulebase can be applied as a fallback value. Fallback is disabled by default.

**Usage Guidelines**

Use this command to configure the default bandwidth policy for a rulebase.

For subscribers using the current rulebase, the default bandwidth policy will be used if in the APN/subscriber profile the `default active-charging bandwidth-policy fallback-enabled` command is configured, or no bandwidth policy is configured.

**Examples**

The following command configures a bandwidth policy named `standard` for the rulebase:

`bandwidth default-policy standard`
billing-records

This command allows you to configure the type of billing to be performed for subscriber sessions.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

```
billing-records { egcdr | radius | rf | udr udr-format udr_format_name | failure-handling-udr-format udr_format_name } +
```

```
no billing-records
```

**no**

If previously configured, deletes the billing-records configuration from the current rulebase.

**egcdr**

Generates an enhanced G-CDR (eG-CDR) for GGSN / P-GW-CDR for P-GW, 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.

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-action command in the ACS Charging Action Configuration Mode.

udr udr-format udr_format_name

Generates UDRs with specified the format on the occurrence of an interim trigger condition, at the end of a subscriber session, or a handoff.

udr_format_name must be the name of an UDR format, and must be an alphanumeric string of 1 through 63 characters.

+

Indicates that more than one of the keywords can be entered in a single command.

Usage Guidelines

Use this command to generate enhanced G-CDRs (eG-CDRs), P-GW-CDR for P-GW, 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.

Examples

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 allows you to specify the Diameter sub-AVPs to be included in the Diameter group AVP "Requested-Service-Unit" sent with DCCA Credit Control Requests (CCRs).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

```
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 } + }
no cca diameter requested-service-unit sub-avp
```

**no**

No sub-AVPs are included in the Requested-Service-Unit grouped AVP.

**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 4000000000.

**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 4000000000.

**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 through 4000000000.

+: Indicates that more than one of the previous keywords can be entered within a single command.

**Usage Guidelines**

Use this command to include sub-AVPs based on time, volume, and service specific unit in the "Requested-Service-Unit" grouped AVP with CCRs through Gy interface.

**Examples**

The following command sets the time based sub-AVP with charging duration of 45 seconds in "Requested-Service-Unit" group AVP on DCCA CCRs:

```
cca diameter requested-service-unit sub-avp time cc-time 45
```
This command allows you to configure various time- and threshold-based quotas in the Prepaid Credit Control Service (Credit Control Application).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

```
cca quota { holding-time holding_time content-id content_id | retry-time retry_time | max-retries retries }
{ default | no } cca quota { holding-time content-id content_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. After `holding_time` seconds has passed without user traffic, the quota is reported back and the charging stops until new traffic starts.

`holding_time` must be an integer from 1 through `4000000000`.

```
content-id content_id
```

Specifies the content ID (Rating group AVP) to use for the Quota holding time for the current rulebase. `content_id` is the content ID specified for credit control service in ACS.

In 12.1 and earlier releases, `content_id` must be an integer from 1 through 65535.

In 12.2 and later releases, `content_id` must be an integer from 1 through 2147483647.

```
retry-time retry_time | max-retries retries |
```

Specifies the retry time for the quota request, in seconds.

`retry_time` must be an integer from 0 through 86400. To disable this assign 0.

Default: 60
This parameter defines the maximum frequency at which the Credit-Control Application (CCA) tries to obtain quota for a subscriber passing traffic for a category with no/exhausted quota.

For a subscriber not passing traffic, the CCA will not try to obtain quota (except once at session start time, if so configured). 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, the 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 a large value for retry-time in quota charging or a top-up scenario.

`max-retries retries` configures the maximum number of retries allowed for blacklisted categories. This option has a default value of 65535 retries (the maximum value).

`retries` must be an integer from 1 through 65535. To disable this assign 0.

**Usage Guidelines**

Use this command to set the prepaid credit control quotas.

`cca quota retry time` allows an 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 the server sends the quota holding time (QHT) it has highest priority to use that QHT regardless of the value configured in the rulebase or Credit Control Application Configuration Mode. QHT configured here has the second priority for the content ID (rating group) configured here.

If the QHT is not available from the server or rulebase configuration mode, the QHT values configured via the Credit Control Application Configuration Mode are used.

**Examples**

The following command configures the prepaid credit control request retry time to 30 seconds:

`cca quota retry-time 30`

The following command specifies the system to use the QHT value configured in the Credit Control Application Mode:

`no cca quota holding-time content-id 1`

The following command specifies the system to ignore the QHT value configured in the Credit Control Application Mode:

`default cca quota holding-time content-id 1`

The following command configures the prepaid credit control request retry time to 60 seconds and the maximum number of retries to 65535:

`default cca quota retry-time max-retries`
**cca quota time-duration algorithm**

This command allows you to specify the algorithm to compute time duration for Prepaid Credit Control Application quotas in the current rulebase.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-rule-base)#
```

**Syntax Description**

```
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

no cca quota time-duration algorithm { consumed-time | continuous-time-periods | parking-meter } [ content-id content_id ]
```

- **no**
  
  If previously configured, deletes the quota time-duration algorithm configuration from the current rulebase.

- **default**

  Configures this command with its default setting.

- **consumed-time seconds**

  Specifies the Quota Consumption Time (QCT) in seconds. QCT is used with active time-based quotas and to determine chargeable time envelopes for consuming time quota.

  `seconds` must be an integer from 1 through 4294967295.

  Default: 0 (disabled)

  A 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**

  Specifies 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**

Specifies the charging quota continuous period, in seconds.

*seconds* must be an integer from 1 through 4294967295.

Default: 0 (disabled)

The Continuous Time Periods (CTP) mechanism constructs time-envelopes from 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 (the one which contained no traffic).

**parking-meter seconds**

Specifies the Parking Meter (PM) period, in seconds, for a particular rating group.

*seconds* must be an integer from 1 through 4294967295.

Default: 0 (disabled)

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).

**content-id content_id**

Specifies the content ID (Rating group AVP) to use for the CCA Quota time duration algorithm selection in the current rulebase.

*content_id* is the content ID specified for credit control service in ACS.

In 12.1 and earlier releases, *content_id* must be an integer from 1 through 65535.

In 12.2 and later releases, *content_id* must be an integer from 1 through 2147483647.

**Usage Guidelines**

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.

**Examples**

The following command configures the QCT to consumed-time duration of 400 seconds:

```
cca quota time-duration algorithm consumed-time 400
```
**cca radius accounting interval**

This command allows you to configure how often interim updates are generated by the RADIUS Credit Control Application to be sent to the prepaid server.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

```
cca radius accounting interval interval
{ default | no } cca radius accounting interval
```

- **default**
  
  Configures the command with its default setting.
  
  Default: Disabled; same as **no cca radius accounting interval**

- **no**

  Disables interim updates.

- **interval**

  Specifies the time interval, in seconds, between interim updates generated by the RADIUS Credit Control Application.

  *interval* must be an integer from 1 through 3600.

  Default: 1 (Disabled)

**Usage Guidelines**

Use this command to specify the RADIUS accounting interval between accounting of a prepaid subscriber. The same parameters are applicable for RADIUS server group.
Examples

The following command defines RADIUS accounting interval of 20 seconds for RADIUS prepaid service in the rulebase:

```
cca radius accounting interval 20
```
**cca radius charging context**

This command allows you to specify the RADIUS servers used for the current rulebase when RADIUS credit control is enabled.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**
```
cca radius charging context vpn_context [ group server_group_name ]
no cca radius charging context
```

`no`
RADIUS credit control will not be performed.

`vpn_context`
Specifies the charging context where RADIUS prepaid charging parameters are configured.
`vpn_context` must be an alphanumeric string of 1 through 79 characters.

`group server_group_name`
Specifies the RADIUS server group.
`server_group_name` must be the name of a RADIUS server group, and must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**
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.

**Examples**
The following command defines RADIUS charging context `prepaid_rad1` for RADIUS prepaid charging in the rulebase:
```
cca radius charging context prepaid_rad1
```
**cca radius user-password**

This command allows you to configure the value to use for the "User-Password" attribute in RADIUS messages sent to the prepaid server.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

```
cca radius user-password | encrypted | password password
no cca radius user-password
```

- **no**
  - If previously configured, deletes the RADIUS prepaid service user password configured in the current rulebase.

- **encrypted | password password**
  - Specifies the password for prepaid services within the current rulebase.
  - In 12.1 and earlier releases, `password` must be an alphanumeric string of 1 through 63 characters with or without encryption.
  - In 12.2 and later releases, `password` must be an alphanumeric string of 1 through 63 characters without encryption, and 1 through 132 characters with encryption enabled.

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 Guidelines**

Use this command to specify the RADIUS user password for prepaid services within the current rulebase.

**Examples**

The following command configures the user password as `user_123` without encryption in the current rulebase:

```
cca radius user-password password user_123
```
charging-action-override

This command allows you to enable/disable overriding charging parameters of static rule with those of an ip-any rule or a specified dynamic rule.

Product

GGSN
P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax Description

charging-action-override custom1 [ use-rule dynamic_rule_name ]
{ default | no } charging-action-override

default

Configures this command with its default setting.

Default: Disables overriding charging parameters of static rule with those of an ip-any or a specified dynamic rule.

no

Disables overriding charging parameters of static rule with those of an ip-any or a specified dynamic rule.

custom1

Specifies overriding Online/Offline, Service ID, Content ID, Flow Control, ARP, and QCI.

use-rule dynamic_rule_name

Optional: Specifies the dynamic rule to inherit charging parameters from. If a dynamic rule name is not specified, the charging properties will be inherited from any dynamic rule.

dynamic_rule_name specifies name of the dynamic rule, and must be an alpha and/or numeric string of 1 through 63 characters in length.
Usage Guidelines

Use this command to enable/disable overriding charging parameters of static rule with those of a dynamic ip-any rule or a specified dynamic rule.

Examples

The following command specifies to enable overriding charging parameters of static rule with those of a dynamic rule named *test*:

```
charging-action-override custom1 use-rule test
```
charging-rule-optimization

This command allows you to configure the internal optimization level to use, for improved performance, when evaluating each instance of the action priority command.

---

**Important**

In StarOS 14.0 and later releases, this command is deprecated. In StarOS 14.0 and later releases, rule optimization is always enabled with the optimization level set to high.

---

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local][host_name](config-rule-base)#
```

**Syntax Description**

charging-rule-optimization { high | low | medium }

default charging-rule-optimization

default

Configures this command with its default setting.

Default: In 11.0 and later releases: **high** In 10.0 and earlier releases: **low**

**Important**

In 11.0 and later releases, the **medium** keyword is deprecated.
Enables medium level of optimization with moderate memory utilization.

**Usage Guidelines**

Use this command to specify the level of internal optimization for improved performance when evaluating each instance of the `action priority` command.

Both the high and medium options cause re-organization of the entire memory structure whenever any change is made, such as on the addition of an `action priority` command.

**Examples**

The following command specifies the highest optimization level for rule search and matching in the rulebase: `charging-rule-optimization high`
check-point accounting

This command configures micro checkpoint syncup timer for ICSR and Session Recovery for Rf-Gy synchronization.

**Product**
- GGSN
- P-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

```
check-point accounting sync-timer \{ icsr | sr \} timer_value \{ sr | icsr \} timer_value
no check-point accounting sync-timer \{ icsr | sr \}
```

- **no**
  - If the micro checkpoint syncup timer is already configured, then the **no** variant will delete the configuration.

- **sr timer_value**
  - Configures micro check-pointing timer for Session Recovery (SR). By default, the session recovery check-pointing will be done on 8 seconds.
  - **timer_value**: Time configured will be in multiples of 2 seconds. Note that the timer value less than 4 seconds and greater than 60 seconds will not be accepted.

- **icsr timer_value**
  - Configures micro check-pointing timer for ICSR. By default, the ICSR check-pointing will be done on 18 seconds.
  - **timer_value**: Time configured will be in multiples of 2 seconds. Note that the timer value less than 4 seconds and greater than 60 seconds will not be accepted.

**Usage Guidelines**

Use this command to configure micro checkpoint syncup timer for ICSR and Session Recovery. Micro Checkpoint Sync-up timer is an internal timer utilized by Rf and Gy modules to check point corresponding billing information.
Releases prior to 17.0, micro checkpoint sync-up timer was hardcoded with a value of 18 seconds for ICSR and 8 seconds for Session Recovery (SR). In 17.0 and later releases, the micro checkpoint sync-up timer is made configurable with an expectation that it be set at a value as low as 4 seconds. The timer value is reduced to ensure the accurate billing information during the ICSR or SR switchover event.

This CLI is available at both active charging service level and rulebase level. If the timer value is configured at both service and rulebase level, then the service level value will be overridden with rulebase level values.

This feature provides the operator with the flexibility to provision timer for accurate billing information in case of session recovery or ICSR switchover. However, this is a performance impacting feature and the impact of the micro checkpoint sync timer reduction needs to be carefully considered by the operator before provisioning a lower value.

**Examples**

The following command configures the micro checkpoint syncup timer for Session Recovery as 8 seconds:

```
check-point accounting sync-timer sr 8
```
constituent-policies

This command allows you to configure the Bandwidth, Content Based Billing (CBB), and Firewall/Firewall-and-NAT constituent policies. The combination of the values of all three policies will uniquely identify the associated rulebase.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

**Syntax Description**

constituent-policies { bandwidth-policy bandwidth_policy_name | cbb-policy cbb_policy_name | firewall-policy fw_policy_name | fw-and-nat-policy fw_nat_policy_name } +

no constituent-policies

no

If previously configured, deletes the constituent-policies configuration from the current rulebase.

**bandwidth-policy bandwidth_policy_name**

Specifies the Bandwidth policy.

*bandwidth_policy_name* must be the name of a bandwidth policy, and must be an alphanumeric string of 1 through 63 characters.

**cbb-policy cbb_policy_name**

Specifies the Content Based Billing (CBB) policy.

*cbb_policy_name* must be the name of a CBB policy, and must be an alphanumeric string of 1 through 63 characters.

**firewall-policy fw_policy_name**

*Important*

This keyword is customer specific. For more information, please contact your Cisco account representative.
Specifies the Stateful Firewall policy.

fw_policy_name must be the name of a Stateful Firewall policy, and must be an alphanumeric string of 1 through 63 characters.

fw-and-nat-policy fw_nat_policy_name

- **Important**: This keyword is customer specific, and is only available in StarOS 8.1 and in StarOS 9.0 and later releases.

Specifies the Firewall-and-NAT policy.

fw_nat_policy_name must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to configure the bandwidth, CBB, and Firewall/Firewall-and-NAT constituent policies that will identify the rulebase. The combination of the values of all three policies will uniquely identify the rulebase associated.

**Examples**

The following command configures the constituent bandwidth policy named test123:

`constituent-policies bandwidth-policy test123`
content-filtering category policy-id

This command allows you to configure the Content Filtering Category Policy Identifier for Policy-based Content Filtering support in the current rulebase.

**Product**

CF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Command Modes

- Exec > ACS Configuration > Rulebase Configuration
- active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

- `content-filtering category policy-id cf_policy_id`
- `no content-filtering category policy-id [ cf_policy_id ]`

**no**

If previously configured, deletes the configuration from the current rulebase.

If StarOS 8.1 and later releases, 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.

- `content-filtering 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**

If 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 that is configured using the `category policy-id cf_policy_id` command in the APN/Subscriber Configuration Mode prevails over this configuration.
**Usage Guidelines**

Use this command to configure the Content Filtering Category Policy ID for Policy-based Content Filtering support in the rulebase.

The Content Filtering Category Policy is created/deleted in the ACS Configuration Mode, and is configured in the Content Filtering Policy Configuration Mode.

**Examples**

The following command configures the Content Filtering Category Policy ID 101 in the rulebase:

```
content-filtering category policy-id 101
```
**content-filtering flow-any-error**

This command allows you to specify action to take on Content Filtering packets in the case of ACS error scenarios.

**Product**

CF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

**active-charging service service_name > rulebase rulebase_name**

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

`content-filtering flow-any-error { deny | permit }`

`default content-filtering flow-any-error`

**default**

Configures this command with its default setting.

Default: `permit`

**deny**

Configures flow-any-error configuration as deny.

All the denied packets will be accounted for by the `discarded-flow-content-id` configuration in the Content Filtering Policy Configuration Mode. This content ID will be used to generate UDRs for packets denied via content filtering.

**permit**

Configures flow-any-error configuration as permit.

**Usage Guidelines**

Use this command to allow/discard content filtering packets in case of ACS error scenarios.

**Examples**

The following command allows content filtering packets in case of an ACS error:

`content-filtering flow-any-error permit`
content-filtering mode

This command allows you to enable/disable the specified Category-based Content Filtering mode in the current rulebase.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-rule-base)#

Syntax Description

countent-filtering mode { category { static-and-dynamic | static-only } | server-group cf_server_group }

no content-filtering mode

no

If previously configured, deletes the content-filtering mode configuration from the current rulebase. Content filtering will not to be performed for the current rulebase. This is the default setting.

category { static-and-dynamic | static-only }

Specifies the Category-based Content Filtering mode.

- **static-only**: Configures Category-based Content Filtering in static only mode, wherein all URLs are compared against an internal database to categorize the requested content. Using Category-based Content Filtering support requires configuration of the require active-charging content-filtering category command in the Global Configuration Mode.

- **static-and-dynamic**: Configures Category-based Content Filtering in Static-and-Dynamic mode, wherein a static rating of the URL is first performed, and only if the static rating fails to find a match, dynamic rating of the content that the server returns is then 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` command.

---

**server-group cf_server_group**

Enables and configures the Content Filtering Server Group (CFSG) mode within the rulebase to manage an external content filtering server with an Internet Content Adaptation Protocol (ICAP) client system.

*cf_server_group* must be the name of a CFSG, and must be unique, and must be an alphanumeric string of 1 through 63 characters.

If configured, ACS attempts to establish TCP connections to every server in the named group.

**Usage Guidelines**

Use this command to enable and apply the content filtering mode in the rulebase to manage a content filtering server with an ICAP client system.

**Examples**

The following command enables the content filtering mode for external content filtering server group *CF_Server1* in the rulebase:

```
content-filtering mode server-group CF_Server1
```

The following command enables the category based static and dynamic content filtering mode for in the rulebase:

```
content-filtering mode category static-and-dynamic
```
credit-control-group

Configures the credit control group to be used for subscribers who use this rulebase.

Product

GGSN
HA
HSGW
IPSG
PDSN
P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

`credit-control-group cc_group_name`

`no credit-control-group`

`no`

Removes the credit-control group configuration from the current rulebase, if previously configured. This is the default setting.

`cc_group_name`

Specifies name of the credit-control group as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to specify the desired CC group whenever the rulebase is selected during the subscriber session setup. This is an optional CLI configuration, and used only when customized Assume Positive behavior is required for subscribers. This CLI configuration is applicable only during the session setup. Mid-session change in the CC group is not allowed.

The `credit-control-group cc-group-name` command is used to specify a credit-control group name association to the rulebase. The `no credit-control-group` CLI is to remove the association. The default setting is `no credit-control-group`. 
If this CLI command is configured, the selection of the CC group is based on the following precedence order.

- PCRF provided CC group
- AAA provided CC group
- Rulebase configured CC group
- Subscriber Profile/APN selected CC group
- Default Credit-Control group

For example, if a CC group is configured in the rulebase then this CC group has higher precedence over the CC group value specified in the Subscriber/APN profile.

If the CC group configuration is not present in the rulebase, the default subscriber/APN profile configuration is applied.

**Examples**

The following command configures the association of a credit-control group named *test* for the current rulebase:

```
credit-control-group test
```
**description**

Allows you to enter descriptive text for this configuration.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
description text
no description
```

- **no**
  
  Clears the description for this configuration.

- **text**
  
  Enter descriptive text as an alphanumeric string of 1 to 100 characters.
  
  If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

**Usage Guidelines**

The description should provide useful information about this configuration.
**dynamic-rule order**

This command allows you to specify whether dynamic rules are matched before statically configured rules.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**

- `dynamic-rule order { always-first | first-if-tied }
- `no dynamic-rule order

`no`

If previously configured, deletes the dynamic-rule order configuration from the current rulebase. By default, dynamic rules are matched against the flow prior to static rules.

- `always-first`
  Specifies to match all the dynamic rules against the flow prior to any static rule.

- `first-if-tied`
  Specifies to match rules against the flow based on their priority with the condition that dynamic rules match before a static rule of the same priority.

A rule is a combination of a ruledef, charging action, and precedence. Static rules are defined by the `action` CLI command in the ACS Rulebase Configuration Mode, and are applicable to all subscribers that are associated with the rulebase. Dynamic rules are obtained via a dynamic protocol, such as, the Gx-interface for a particular subscriber session.

**Usage Guidelines**

Use this command to configure the order in which rules are selected for matching in between dynamic rules (per subscriber) and static rules (from rulebase).

**Examples**

The following command matches all dynamic rules against the flow prior to any static rule:

```
dynamic-rule order always-first
```
**edr edr-dcca-fh**

This command configures generation of EDRs when the OCS is in unreachable state.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

*active-charging service* service_name > *rulebase* rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

**Syntax Description**

`edr edr-dcca-fh [ charging-edr charging_edr_format_name | edr-format edr_format_name | reporting-edr reporting_edr_format_name ] + { default | no } edr edr-dcca-fh`

`default`

Configures this command with its default setting.

Default: Disabled

`no`

If previously configured, deletes the configuration from the current rulebase.

`charging-edr charging_edr_format_name`

Specifies to generate charging EDR during OCS unreachable period.

*charging_edr_format_name* must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

`edr-format edr_format_name`

Specifies to generate EDR during OCS unreachable period.

*edr_format_name* must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.
reporting-edr reporting_edr_format_name

Specifies to generate reporting EDR during OCS unreachable period.

`reporting_edr_format_name` must be the name of a reporting EDR format, and must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to configure the trigger to generate EDRs when the OCS is in unreachable state. This configuration provides the facility to track and report the actual quota usage through EDRs during Assume Positive scenarios for HA.

This feature has been enhanced to support reporting / recording the appropriate usage in volume and time during regular OCS sessions and during assume positive scenarios separately. In this release, EDRs will be generated with new closure reasons when OCS goes down for HA.

**Examples**

The following command configures the generation of charging EDRs when OCS is unreachable:

```
edr edr-dcca-fh charging-edr edr1
```
edr p2p

This command configures generation of Event Detail Records (EDR) for P2P events. This command is associated with the Dynamic Software Upgrade process.

Product
ACS
ADC

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax Description

edr p2p p2p_event_list | charging-edr charging_edr_format_name | edr-format edr_format_name | reporting-edr reporting_edr_format_name | +
{ default | no } edr p2p p2p_event_list

default
Configures this command with its default setting.
Default: Disabled

no
If previously configured, deletes the configuration from the current rulebase.

p2p_event_list
Specifies the name of the P2P EDR Event. The plugin supports only the "audio-end" and "video-end" events. This P2P event list can be any P2P event that is supported by the plugin.
p2p_event_list must be an alphanumeric string of 1 through 128 characters.

charging-edr charging_edr_format_name
Specifies to generate charging EDR for P2P events.
charging_edr_format_name must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.
edr-format **edr_format_name**

Specifies to generate EDR for P2P events.

*edr_format_name* must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.

**reporting-edr** **reporting_edr_format_name**

Specifies to generate reporting EDR for P2P events.

*reporting_edr_format_name* must be the name of a reporting EDR format, and must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to configure the P2P events to generate EDRs. The list of P2P events will be populated from the currently loaded plugin.

A plugin is a functional software entity that provides incremental updates to a pre-existing StarOS software component. Plugins can be dynamically loaded at runtime and do not require a system restart. For more information on the Dynamic Software Upgrade feature, refer to *Application Detection and Control Administration Guide*.

**Examples**

The following command configures the generation of EDRs for P2P *audio-end* event specifying to use the EDR format named *edr1*:

```
edr p2p audio-end edr-format edr1
```
edr nemo-call

This command enables/disables the NEMO feature for populating the EDRs with source IP, destination IP and VRF name of the NEMO Mobile Router (MR) host.

**Important**

This CLI command is available only with NEMO license. Contact your Cisco account representative for more information.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**

`[ default | no ] edr nemo-call`

- **default**
  
  Configures this command with its default setting.
  
  Default: Disabled

- **no**
  
  If previously configured, deletes the configuration from the current rulebase.

- **nemo-call**
  
  This keyword controls the feature of populating the EDRs with source IP, destination IP and VRF name associated with UEs behind the NEMO MRs.

  By default this keyword option will be disabled i.e. this CLI should be configured if the feature needs to be turned ON.

**Usage Guidelines**

Use this command to enable this feature of creating the EDRs with the source IP, destination IP and VRF name of the NEMO host.
This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Important

Releases prior to 18.0, ECS did not see the inner user packet i.e. it sees only MIP packet containing user data in both uplink and downlink direction. For example, it sees [IP header1][GRE header][IP header2][payload]. In 18.0 and later releases, ECS will see and analyze the inner IP packets i.e. [IP header2][payload], and determine the source IP, destination IP and VRF name of the NEMO hosts.

Examples

The following command enables the generation of EDRs with source IP, destination IP and VRF name of the NEMO host:

`edr nemo-call`
edr sn-charge-volume

This command allows you to exclude/include packets/bytes that are dropped/retransmitted by the ACS in the total charge volume — "sn-charge-volume" EDR attribute.

**Important**

In release 17.0, this command has been deprecated. This configuration is available at rulebase level as

```
```

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**

```
[ default | no ] edr sn-charge-volume { count-dropped-units | count-retransmitted-units }
```

**default**

Configures this command with its default setting.

Default: Exclude, in the total charge volume, packets/bytes dropped/retransmitted by ACS.

**no**

Exclude, in the total charge volume, packets/bytes dropped/retransmitted by ACS.

**count-dropped-units**

Specifies to include dropped units in the total charge volume.

**count-retransmitted-units**

Specifies to include retransmitted units in the total charge volume.

**Usage Guidelines**

Use this command to exclude/include packets/bytes that are dropped/retransmitted by ACS in the total charge volume — "sn-charge-volume" EDR attribute.
This command applies only to the "sn-charge-volume" attribute and does not affect the "sn-volume-amt" counts in any way.

**Examples**

The following specifies to include units retransmitted by ACS in the sn-charge-volume EDR attribute:

```
edr sn-charge-volume count-retransmitted-units
```
edr suppress-zero-byte-records

This command disables/enables the creation of EDRs when there is no data for the flows.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Rulebase Configuration
active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-rule-base)#

Syntax Description
[ default | no ] edr suppress-zero-byte-records

default
Configures this command with its default setting.
Default: Disabled; same as no edr suppress-zero-byte-records

no
Disables the suppression of zero-byte EDRs.

edr suppress-zero-byte-records
Suppresses zero-byte EDRs.

Usage Guidelines
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.
edr transaction-complete

This command enables/disables the generation of an EDR on the completion of a transaction.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**

```
edr transaction-complete http [ charging-edr charging_edr_format_name | edr-format edr_format_name | reporting-edr reporting_edr_format_name ] [ default | no ]
```

- **default**
  Configures this command with its default setting.
  Default: Disabled; same as **no edr transaction-complete**

- **no**
  If previously configured, deletes the configuration from the current rulebase.

- **http**
  - **http**: HTTP protocol related configuration

- **edr-format edr_format_name**
  Specifies to generate EDR on transaction completion for HTTP protocol.
  `edr_format_name` must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.

- **charging-edr charging_edr_format_name**
  Specifies to generate charging EDR on transaction completion.
charging_edr_format_name must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

reporting-edr reporting_edr_format_name

Specifies to generate reporting EDR on transaction completion.

reporting_edr_format_name must be the name of a reporting EDR, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure the generation of an EDR when certain application transactions (for example, request/response pairs) complete. EDR generation is supported for HTTP protocol. Note that these EDRs are in addition to those that might be generated due to other conditions, for example, EDR configurations in a Charging Action.

Examples

The following command configures the generation of charging EDRs on the completion of transactions for HTTP protocol specifying the EDR format as test123:

```
edr transaction-complete http charging-edr test123
```
edr voip-call-end

This command enables/disables generation of EDRs on the completion of Voice over IP (VoIP) calls. This command is no longer supported for ADC in 14.0 and later releases.

**Product**

ACS

ADC

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-rule-base) #

**Syntax Description**

In StarOS 12.2 and later releases:

```
edr voip-call-end { charging-edr charging_edr_format_name | edr-format edr_format_name | reporting-edr reporting_edr_format_name } +
{ default | no } edr voip-call-end
```

In StarOS 12.1 and earlier releases:

```
edr voip-call-end edr-format edr_format_name
{ default | no } edr voip-call-end
```

default

Configures this command with its default setting.

Default: Disabled; same as no edr voip-call-end

no

If previously configured, deletes the edr voip-call-end configuration from the current rulebase.

```
edr-format edr_format_name
```

**Important**

This option is available only in 12.1 and earlier releases. In 12.2 and later releases, it has been deprecated and is replaced by the charging-edr option.

Specifies to generate an EDR when a VoIP call ends.
**edr_format_name** must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.

**charging-edr charging_edr_format_name**

**Important** This option is available only in 12.2 and later releases.

Specifies to generate a charging EDR when a VoIP call ends.

*charging_edr_format_name* must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

**reporting-edr reporting_edr_format_name**

**Important** This option is available only in 12.2 and later releases.

Specifies to generate a reporting EDR when a VoIP call ends.

*reporting_edr_format_name* must be the name of a reporting EDR format, and must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to generate an EDR on the completion of voice calls. Note that these EDRs are in addition to those that might be generated due to other conditions, for example EDR configurations in a Charging Action. This command facilitates P2P voice duration reporting.

**Examples**

In 12.1 and earlier releases, the following command specifies generating EDRs on completion of VoIP calls using the EDR format *test13*:

```
edr voip-call-end edr-format test13
```

In 12.2 and later releases, the following command specifies generating charging EDRs on completion of VoIP calls using the EDR format named *test23*:

```
edr voip-call-end charging-edr test23
```
egcdr inactivity-meter

**Description** This command has been deprecated. It is included in the CLI for backward compatibility with older configuration files. When executed performs no function. Use the `egcdr threshold interval interval [regardless-of-other-triggers]` command for this functionality.
egcdr cdr-encoding

This command allows you to configure the eG-CDR encoding type.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**
`egcdr cdr-encoding { ascii | delimiter { colon | comma | pipe } } | asn.1 }

default eegcdr cdr-encoding`

- **default**
  Configures the default eG-CDR CDR-encoding format.
  Default: `asn.1`

  - `ascii | delimiter { colon | comma | pipe }`:
    Specifies to use ASCII encoding type to generate eG-CDR in ASCII format.

    - **delimiter { colon | comma | pipe }**: Specifies the delimiter character to use in eG-CDRs in ASCII format.
      - `colon`: Specifies to use ":" (colon) as a delimiter in eG-CDR.
      - `comma`: Specifies to use "," (comma), as a delimiter in eG-CDR.
      - `pipe`: Specifies to use ":" (pipe) as a delimiter in eG-CDR.

    Default: `pipe`

  - `asn.1` specifies to use ASN.1 encoding type to generate eG-CDR in ASN.1 format.

    This is the default setting.

**Usage Guidelines**
Use this command to configure the eG-CDR encoding type.
For more information on using eG-CDR ASCII encoding type in your deployment, contact your Cisco account representative.

**Examples**

The following command specifies to use ASCII encoding type to generate eG-CDR in ASCII format while specifying the delimiter character as comma:

```
egcdr cdr-encoding ascii delimiter comma
```
egcdr tariff

This command allows you to configure the eG-CDR tariff time to generate new eG-CDRs for GGSN and P-GW-CDRs for P-GW.

Product

- GGSN
- P-GW
- SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name{config-rule-base}#

Syntax Description

| no | egcdr tariff minute minute hour hour |

| no |
| If previously configured, deletes the configuration from the current rulebase. |

| minute minute |
| Specifies the minute for the time-of-day configuration. |
| minute must be an integer from 0 through 59. |

| hour hour |
| Specifies the hour for the time-of-day configuration. |
| hour must be an integer from 0 through 23. |

Usage Guidelines

Use this command to configure the eG-CDR tariff time to generate new eG-CDRs for GGSN and P-GW-CDRs for P-GW. Up to four different time-of-day settings may be configured. When any configured tariff time is reached, the current eG-CDR/P-GW-CDR will be closed and a new eG-CDR/P-GW-CDR is opened.
The following command defines an eG-CDR tariff for the 23rd minute of the 22nd hour of the day (10:23 PM):

```
egcdr tariff minute 23 hour 22
```
egcdr threshold

This command allows you to configure the thresholds for generating eG-CDRs for GGSN and P-GW-CDRs for P-GW.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

```
gecdr threshold { interval interval [ regardless-of-other-triggers ] | volume { downlink | total | uplink } bytes } 
{ default | no } egcdr threshold { interval | volume } 

no
```

If previously configured, deletes the eG-CDR threshold configuration from the current rulebase.

```
default
```

Configures this command with the default settings.

Default: Disabled; same as `no egcdr threshold interval` and `no egcdr threshold interval volume` commands.

```
interval interval [ regardless-of-other-triggers ]
```

Specifies the time interval, in seconds, for closing the eG-CDR/P-GW-CDR if the minimum time duration thresholds are satisfied.

`interval` must be an integer from 60 through 40000000.

**regardless-of-other-triggers:** This option enables eG-CDR/P-GW-CDR generation at the fixed time interval irrespective of any other eG-CDR/P-GW-CDR triggers that may have happened in between.

Default: Disabled.
volume { downlink | total | uplink } bytes

Specifies the uplink/downlink volume octet counts for the generation of the interim eG-CDRs/P-GW-CDRs.

- **downlink bytes**: Specifies the limit for the number of downlink (from network to subscriber) octets after which the eG-CDR/P-GW-CDR is closed.
  
  `bytes` must be an integer from 100000 through 4000000000.
  
  Default: 4000000000

- **total bytes**: Specifies the limit for the total number of octets (uplink+downlink) after which the eG-CDR/P-GW-CDR is closed.
  
  `bytes` must be an integer from 100000 through 4000000000.
  
  Default: Disabled

- **uplink bytes**: Specifies the limit for the number of uplink (from subscriber to network) octets after which the eG-CDR/P-GW-CDR is closed.
  
  `bytes` must be an integer from 100000 through 4000000000.
  
  Default: 4000000000

**Usage Guidelines**

Use this command to configure thresholds to generate eG-CDRs/P-GW-CDRs.

Thresholds can be specified for both time interval and for data volume, by entering the command twice (once with interval and once with volume). When either configured threshold is reached, the eG-CDR/P-GW-CDRs will be closed. The volume trigger can be specified for uplink or downlink or combined total (uplink + downlink) byte thresholds. The exact keyword forces the configured volume to exactly match the volume in the eG-CDR/P-GW-CDRs, so the triggering packet might have to be divided across two eG-CDRs/P-GW-CDRs.

When both interval and volume triggers are configured, we'll reset the interval time and accumulated volume amount whenever the eG-CDR/P-GW-CDRs is closed regardless of whether it was due to the interval time expiration or reaching the volume limit. Use the regardless-of-other-triggers optional keyword, if you want the eG-CDRs/P-GW-CDRs closed at the configured regular intervals, regardless of whether eG-CDRs/P-GW-CDRs are being closed due to reaching a volume limit.

When the PDP context is terminated, the eG-CDR/P-GW-CDRs will be closed regardless of whether the thresholds have been reached.

**Examples**

The following command defines an eG-CDR threshold interval of 600 seconds:

```
egcdr threshold interval 600
```
egcdr time-duration algorithm

This command allows you to specify the algorithm to compute the duration of time utilization in an eG-CDR for the current rulebase.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax Description

egcdr time-duration algorithm { consumed-time consumed_time [ plus-idle ] | continuous-time-periods ctp_time | parking-meter seconds } { default | no } egcdr time-duration algorithm

no

If previously configured, deletes the eG-CDR time-duration algorithm configuration from the current rulebase.

default

Configures this command with its default setting.

Default: Algorithm configured for CCA, or the CCA default if none is configured.

consumed-time consumed_time [ plus-idle ]

Specifies the actual consumption time in seconds. This is used to determine the actual used chargeable time envelopes for the purpose of consuming time quota.

consumed_time must be an integer from 1 through 4294967295.

Default: 0 (disabled)

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.

plus-idle: Specifies 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**

Specifies 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 the first packet and thereafter include only that period in charging in which one or more packets arrived. For the period where no packets arrived or no traffic was detected, usage will not be computed.

ctp_time must be an integer from 1 through 4294967295.

**parking-meter seconds**

Specifies the Parking Meter (PM) period, in seconds.

seconds must be an integer from 1 through 4294967295.

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 is set to 300 seconds (5 minutes) and the subscriber only uses one minute, the charge is for 5 minutes.

**Usage Guidelines**

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).

**Examples**

The following command sets consumed time duration to 400 seconds:

```bash
egcdr time-duration algorithm consumed-time 400
```
end

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

`end`

**Usage Guidelines**

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 Description**
exit

**Usage Guidelines**
Use this command to return to the parent configuration mode.
**extract-host-from-uri**

This command allows you to configure whether to use the host name embedded in the URI as the host field, when the host field option in the HTTP or Wireless Session Protocol (WSP) header is absent.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**

`extract-host-from-uri { http | wsp } + { default | no } extract-host-from-uri`

- **default**
  
  Configures this command with its default setting.
  
  Default: Disabled; same as `no extract-host-from-uri`

- **no**
  
  If previously configured, disables the extract-host-from-uri configuration, for both HTTP and WSP, from the current rulebase.

- **http | wsp**
  
  Specifies the protocol(s).

- **+**
  
  Indicates that more than one of the previous keywords can be entered within a single command.

**Usage Guidelines**

If the host field is not present in HTTP/WSP header, this command will extract host from the URI, and store it in the host field to enable "http host" and "wsp host" rule matches using the stored value.
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.

**Examples**

The following command configures extraction of host from URI for both HTTP and WSP protocols:

```
extract-host-from-uri http wsp
```
firewall dos-protection

This command allows you to configure Stateful Firewall 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 releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**

```
[ 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

default

If previously enabled, disables Stateful Firewall protection for subscribers from all or specified DoS attack(s).

```
default
```

Configures this command with its default setting.

Default: Protection from all DOS attacks is disabled.

```
all
```

Enables protection against all DoS attacks supported by the Stateful Firewall in-line service.

```
flooding { icmp | tcp-syn | udp }
```

Enables protection against specified flooding attacks:
- **icmp**: Enables protection against ICMP Flood attacks
- **tcp-syn**: Enables protection against TCP SYN Flood attacks
- **udp**: Enables protection against UDP Flood attacks

**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 Guidelines**

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**

The DoS attacks are detected only in the downlink direction.

**Examples**

The following command enables Stateful Firewall protection from all supported DoS attacks:

```
firewall dos-protection all
```
**firewall flooding**

This command allows you to configure Stateful 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 releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

---

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

**active-charging service service_name > rulebase rulebase_name**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**

```
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 this command the default setting for the specified keyword.

**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

**Usage Guidelines**

Use this command to configure the maximum number of ICMP, TCP-SYN, / UDP packets allowed to prevent the packet flooding attacks to the host.

**Examples**

The following command ensures a subscriber will not receive more that 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 allows you to configure 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 releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

*active-charging service service_name > rulebase rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

```
firewall icmp-destination-unreachable-message-threshold messages then-block-server
{ default | no } firewall icmp-destination-unreachable-message-threshold
```

**default**

Configures this command with its default setting.

Default: No limit

**no**

If previously configured, deletes the configuration from the current rulebase.

**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 Guidelines  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.

Examples  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 allows you to configure the maximum IP packet size (after IP reassembly) allowed over Stateful 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 releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

---

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

```
firewall max-ip-packet-size packet_size protocol { icmp | non-icmp }
default firewall max-ip-packet-size protocol { icmp | non-icmp }
```

**default**

Configures the default maximum IP packet size configuration.

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 Guidelines

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".

Examples

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 allows you to configure Stateful Firewall protection from Multipurpose Internet Mail Extensions (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 releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

---

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

```
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 this command with its 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 Guidelines
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.

Examples
The following command sets the maximum number of headers allowed in an HTTP packet to 100:
\texttt{firewall mime-flood http-headers-limit 100}

The following command sets the maximum header field size allowed in the HTTP header to 1000 bytes:
\texttt{firewall mime-flood max-http-header-field-size 1000}
**firewall no-ruledef-matches**

This command allows you to configure the default action for packets when no Stateful Firewall ruledef matches.

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 releases, 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**
- PSF
- NAT

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > ACS Configuration > Rulebase Configuration
- `active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**

```
firewall no-ruledef-matches { downlink | uplink } action { deny [ charging-action charging_action_name ] | permit [ bypass-nat | nat-realm nat_realm_name ] }
```

`default`:

Configures the default action for packets with no Stateful Firewall ruledef match.

`downlink | uplink`

Specifies the packet type:

- **downlink**: Downlink (from network to subscriber) packets with no Stateful Firewall ruledef match.
  - Default: deny
- **uplink**: Uplink (from subscriber to network) packets with no Stateful Firewall ruledef match.
  - Default: permit
action { deny [ charging-action charging_action_name ] | permit [ bypass-nat | nat-realm nat_realm_name ] }

Specifies the default action for packets with no Stateful Firewall ruledef match.

permit [ bypass-nat | nat-realm nat_realm_name ]: Permit packets.

**Important**  
The bypass-nat keyword is only available in StarOS 8.3 and later releases.

Optionally specify:

- *bypass-nat*: Specifies to bypass Network Address Translation (NAT).
- *nat-realm nat_realm_name*: Specifies a NAT realm to be used for performing NAT on subscriber packets.

*nat_realm_name* must be the name of a NAT realm, and must be an alphanumeric string of 1 through 31 characters.

**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-realm option.

deny [ charging-action charging_action_name ]: Denies specified packets.

Optionally, a charging action can be specified.

*charging_action_name* must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**  
Use this command to configure the default action to be taken on packets with no Stateful 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 Stateful 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.

- Stateful Firewall ruledef matching is done. If a rule matches, the packet is allowed or dropped as per the firewall priority configuration.

- If no Stateful Firewall ruledef matches, the packet is allowed or dropped as per the no-ruledef-matches configuration.

For a packet dropped due to Stateful 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 Stateful 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.

**Examples**

The following command configures Stateful Firewall to permit downlink packets with no ruledef matches:

`firewall no-ruledef-matches downlink action permit`
firewall policy

This command allows you to enable/disable Stateful Firewall support for all subscribers using the current 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 releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-rule-base) #

Syntax Description

firewall policy firewall-required

{ default | no } firewall policy

default

Configures this command with its default setting.

Default: Stateful Firewall support is disabled for all subscribers using the current rulebase.

no

If previously enabled, disables Stateful Firewall support for all subscribers using the current rulebase.

firewall-required

Enables Stateful Firewall support for all subscribers using the current rulebase.

Usage Guidelines

Use this command to enable/disable Stateful Firewall support for all subscribers using the current rulebase.
Examples

The following command enables Stateful Firewall support:

```plaintext
firewall policy firewall-required
```

The following command disables Stateful Firewall support:

```plaintext
no firewall policy
```
**firewall priority**

This command allows you to add and specify the priority and type of a Stateful Firewall ruledef in the current rulebase, and allows you 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 releases, for Policy-based Firewall-and-NAT configuration, use the *access-rule priority* command available in the Firewall-and-NAT Policy Configuration Mode.

---

**Product**

PSF

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**

```
firewall priority priority | dynamic-only | static-and-dynamic | firewall-ruledef firewall_ruledef_name { 
{ deny | charging-action charging_action_name } ] | { permit | nat-realm nat_realm_name | trigger open-port { aux_port_number | range start_port_number to end_port_number } direction { both | reverse | same } ] [ ] } } 
no firewall priority priority
```

**no**

If previously configured, deletes the specified Stateful Firewall ruledef priority configuration from the current rulebase.

**priority**

Specifies the Stateful Firewall ruledef's priority in the current rulebase.

*priority* must be a unique value in the current rulebase, and must be an integer from 1 through 65535.
**firewall-ruledef firewall_ruledef_name**

Specifies the Stateful Firewall ruledef to add to the rulebase. Optionally, the Stateful 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_name** must be the name of a Stateful Firewall ruledef, and must be an alphanumeric string of 1 through 63 characters.

**deny [ charging-action charging_action_name ]**

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 Stateful Firewall ruledefs, only the terminate-flow action is applicable, if configured in the specified charging action.

**charging_action_name** must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

**permit [ nat-realm nat_realm_name | bypass-nat | trigger open-port { aux_port_number | range start_port_number to end_port_number } ]**

Permits packets.

- **nat-realm nat_realm_name**: Specifies the NAT realm to be used for performing NAT on subscriber packets matching the Stateful 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 Stateful Firewall ruledef with no NAT realm name configured.

- **nat_realm_name** must be the name of a NAT realm, and must be an alphanumeric string of 1 through 31 characters.

- **bypass-nat**: Specifies that packets bypass 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 Stateful 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 Guidelines**

Use this command to add Stateful Firewall rulesets 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 Stateful Firewall rules to be applied on the calls. The rulesets 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, an 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 Stateful Firewall rulesets, only the terminate-flow action is applicable if configured in the specified charging action.

For a packet dropped due to Stateful Firewall ruleset 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 Stateful 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.

### Examples

The following command assigns a priority of 10 to the Stateful 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:

```plaintext
firewall priority 10 firewall-ruledef fw_rule1 permit trigger open-port range 100 to 200 direction both
```

The following command configures the Stateful Firewall ruledef *fw_rule2* as a dynamic ruledef:

```plaintext
firewall priority 7 dynamic-only firewall-ruledef fw_rule2 deny
```
firewall tcp-first-packet-non-syn

This command allows you to configure the action to take on TCP flows 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 releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base) #
```

**Syntax Description**

```
firewall tcp-first-packet-non-syn { drop | reset }
```

`default firewall tcp-first-packet-non-syn`

`default`

Configures this command with its default setting.

Default: drop

`drop`

Specifies to drop the packet or session.

`reset`

Specifies to send reset.

**Usage Guidelines**

Use this command to configure action to take on TCP flow starting with a non-syn packet.

**Examples**

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 allows you to configure the Stateful Firewall action to be taken on TCP idle timeout expiry.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.</td>
</tr>
</tbody>
</table>

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

*active-charging service service_name* > *rulebase rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-rule-base) #
```

**Syntax Description**

```
firewall tcp-idle-timeout-action { drop | reset }
default firewall tcp-idle-timeout-action
```

**default**

Configures this command with its default setting.

Default: reset

**drop**

Specifies to drop the packet or session on TCP timeout expiry.

**reset**

Specifies to send reset on TCP timeout expiry.

**Usage Guidelines**

Use this command to configure action to take on TCP idle timeout expiry.

**Examples**

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 allows you to configure 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.

This command is only available in StarOS 8.3 and later releases. In StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration
active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**

```
firewall tcp-reset-message-threshold messages then-block-server
{ default | no } firewall tcp-reset-message-threshold

default
Configures this command with its default setting.
Default: no firewall tcp-reset-message-threshold

no
If previously configured, deletes the firewall tcp-reset-message-threshold configuration from the current rulebase.

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 Guidelines

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.

Examples

The following command sets the threshold on the number of TCP reset messages to 10:

```bash
firewall tcp-reset-message-threshold 10 then-block-server
```
firewall tcp-syn-flood-intercept

This command allows you to configure 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 releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product
PSF

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Rulebase Configuration
active-charging service service_name > rulebase rulebase_name
Entering the above command sequence results in the following prompt:
[local] host_name(config-rule-base)#

Syntax Description
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.

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. Stateful Firewall passively watches to see if TCP connections become established within a configurable interval. If connections are not established within the timeout period, 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 Guidelines**

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.

**Examples**

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 allows you to specify the charging action to be used for packets dropped by Stateful Firewall due to any error conditions.

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

**Syntax Description**

```
flow any-error charging-action charging_action_name
default flow any-error
```

**default**

Configures the default action for packets dropped by Stateful Firewall due to any errors.

Default: Update the flow statistics if flow is available

**charging_action_name**

Specifies the charging action based on which accounting action is taken on packets dropped by Stateful Firewall due to any errors.

charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

**Important**

The charging action specified here should preferably not be used for action on packets dropped due to Stateful 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.
Usage Guidelines

Use this command to configure the charging action for packets dropped by Stateful 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 DoS protection causing the packet to be discarded, and so on.

For a packet dropped due to Stateful Firewall rule def 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-rule def-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-rule def-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, an Event Data Record (EDR) is generated.
- If the content ID is configured, Usage Data Record (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.

Examples

The following command specifies the charging action `test2` for accounting action on packets dropped/discarded by Stateful Firewall due to any error:

`flow any-error charging-action test2`
flow control-handshaking

This command allows you to specify how to charge for the control traffic associated with an application.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**

```
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 ]
```

**Syntax Description**

- `flow control-handshaking { charge-to-application { [ all-packets ] [ initial-packets ] [ mid-session-packets ] [ tear-down-packets ] } | charge-separate-from-application }`:
  - Configures the charging action to include the flow control packets either during initial handshaking only or specified control packets during session for charging.

- `default flow control-handshaking`:
  - Configures this command with its default setting.
  - Default: Same as `no flow control-handshaking`

- `no flow control-handshaking [ charge-to-application ]`:
  - Deletes the flow control-handshaking configuration from the current rulebase. The control packets will use whatever content-id is determined by the normal use of the `action` commands.

  In this command, the optional keyword `charge-to-application` is deprecated and has no effect.

- `charge-to-application { [ all-packets ] [ initial-packets ] [ mid-session-packets ] [ tear-down-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.

  - 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**

Configures the charging action to separate the charging of the initial control packets or all subsequent control packets from regular charging.

**Usage Guidelines**

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 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 command also affects applications that do not use TCP but use other methods for control packets, for example WAP, where WTP/UDP may be used to set up and tear down connection-oriented WSP.

**Examples**

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 allows you to configure the end condition of the session flows related to a user session and triggers EDR generation.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**

```
flow end-condition { content-filtering | hagr | handoff | normal-end-signaling | session-end |
tethering-signature-change | url-blacklisting | timeout } [ flow-overflow ] + { charging-edr
charging_edr_format_name | reporting-edr reporting_edr_format_name }
```

- **no**
  If previously configured, deletes the flow end-condition configuration from the current rulebase.

- **content-filtering**
  Creates an EDR with the specified EDR format whenever a flow ends due to Category-based Content Filtering in-line service action. Possible actions include redirect-url, terminate-flow, content-insert.

- **hagr**
  Creates an EDR with the specified EDR format whenever a flow is terminated due to Inter-chassis Session Recovery action.

- **handoff**
  Creates an EDR with the specified EDR format whenever a flow ends due to hand-off. Whenever a handoff occurs, ACS closes the EDRs for all current flows using the specified EDR format, and begins new statistics collection for the flows for the EDRs that will be generated when the flows actually end.
normal-end-signaling
Creates an EDR with the specified EDR format whenever flow end is signaled normally, for example 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 specified EDR format.

session-end
Creates an EDR with the specified EDR format whenever a subscriber session ends. By this option ACS creates an EDR with the specified format name for every flow that has had any activity since last EDR was created for the flow on session end.

tethering-signature-change
Creates an EDR with specified EDR format for tethering signature change of a flow because of mid flow SYN packets.
Whenever a tethering signature change occurs, ACS closes the EDR with the specified closure reason and begins new statistics collection for the flow. If enabled, flow statistics may get split across multiple EDRs of the flow if tethering signature change occurs.
The maximum limit for tethering signature change detection depends on the tethering-detection max-syn-packet-in-flow CLI command. EDR/REDR generation for tethering signature change is also dependent on this CLI configuration.

url-blacklisting
Creates an EDR with the specified EDR format whenever a flow ends due to URL Blacklisting action.

timeout
Creates an EDR with the specified EDR format whenever a flow ends due to a timeout condition.

flow-overflow

Important This keyword is applicable only when used with the hagr, handoff, tethering-signature-change, and session-end keywords.

Creates an EDR with the specified EDR format whenever there is a flow-overflow condition. If any of the specified end-conditions that affect subscriber information stored at ACS (such as call line) is configured, the "flow-overflow" EDR is generated.

+ Indicates that more than one of the keywords can be entered within a single command.

charging-edr charging_edr_format_name
Specifies the charging EDR format.
 charging_edr_format_name must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.
**reporting-edr reporting_edr_format_name**

Specifies the reporting EDR format.

*reporting_edr_format_name* must be the name of a reporting EDR format, and must be a unique alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to enable or disable the capturing of EDRs based on flow end condition.

**Examples**

The following command configures the flow end condition as handoff and creates a charging EDR with format named *EDR_format1*:

```
flow end-condition handoff charging-edr EDR_format1
```
flow limit-across-applications

This command allows you to limit 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**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

**Syntax Description**

flow limit-across-applications { limit | non-tcp limit | tcp limit }

no flow limit-across-applications { limit | non-tcp limit | tcp limit }

If previously configured, deletes the flow limit-across-applications configuration from the current rulebase.

**flow limit-across-applications limit**

Specifies the maximum number of flows across all applications for the 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 Guidelines

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 ACS Charging Action Configuration Mode set to `no`.

Examples

The following command defines the maximum number of 200000 flows for the rulebase:

```bash
flow limit-across-applications 200000
```
## flow rtsp-all-pkts

This command allows you to delay charge packets in an RTSP flow.

### Product
ACS

### Privilege
Security Administrator, Administrator

### Command Modes
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

### Syntax Description
```
| no | default | flow rtsp-all-pkts charge-to-application |
```

**no**
If previously configured, deletes the flow rtsp-all-pkts configuration from the current rulebase.

**default**
Configures this command with its default setting.

Default: Same as **no flow rtsp-all-pkts charge-to-application**.

**flow rtsp-all-pkts charge-to-application**

Configures delay charging for RTSP traffic. When this configuration is enabled, all packets (TCP control packets and RTSP packets) prior to the RTSP SETUP will be charged to application as per the application ruledef. In other words, they will be charged to the content-id established by the first SETUP of the RTSP flow.

### Usage Guidelines
Use this command to delay charge packets in a RTSP flow. All initial packets (TCP control packets (all packets including initial, mid-session, end-session) and RTSP packets prior to the first SETUP) can be delay charged. Apart from the initial packets, all intermittent TCP control packets are also charged to the last matched Ruledef for the given RTSP flow. This command is used in conjunction with the **rtsp initial-bytes-limit RTSP_bytes** command.
Examples

The following command enables the RTSP flow's delay charging:

```
flow rtsp-all-pkts charge-to-application
```
**fw-and-nat default-policy**

This command allows you to configure the default Firewall-and-NAT policy for the current rulebase. This command must be used to configure the Policy-based Firewall-and-NAT feature.

---

**Important**

This command is only available in StarOS 8.1 and StarOS 9.0 and later releases.

---

**Product**

- PSF
- NAT
- SaMOG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

```plaintext
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

```plaintext
fw-and-nat default-policy fw_nat_policy_name
no fw-and-nat default-policy
```

- **no**
  
  If previously configured, deletes the Firewall-and-NAT default policy configuration from the current rulebase.

- **fw_nat_policy_name**
  
  Specifies the default Firewall-and-NAT policy for the current rulebase.

  `fw_nat_policy_name` must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to configure the default Firewall-and-NAT policy for a rulebase.

For subscribers using the current rulebase, the default Firewall-and-NAT policy will be used if in the APN/subscriber profile the default `fw-and-nat policy` command is configured, and a policy to use is not received from the AAA/OCS.

For more information, see the *Personal Stateful Firewall Administration Guide*. 
Examples

The following command configures a Firewall-and-NAT policy named *standard* to the rulebase:

```
fw-and-nat default-policy standard
```
http header-parse-limit

This command allows you to configure the HTTP header parse limit, on exceeding which the flow is marked as permanent failure and is matched and charged against http error = TRUE ruledef.

Important
This command is customer specific. For more information contact your Cisco account representative.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax Description
http header-parse-limit parse_limit_bytes

{ default | no } http header-parse-limit

default
Configures the default setting for this command.
Default: 12000 bytes

no
If enabled, disables the header-parse-limit configuration in the current rulebase.

Important
Disabling header parse limit may lead to uncharged bytes (due to no rule-matching until header is complete) if header is not correctly terminated.

parse_limit_bytes
Specifies the header-parse-limit, number of bytes.
parse_limit_bytes must be an integer from 1 through 256000.
Usage Guidelines

If a user sends HTTP LF terminated traffic instead of the usual HTTP CRLF terminated traffic, and similarly
the server is responding with LF terminated traffic, the traffic does not result in any rule match, and rule match
happens only at flow idle or at call clear when the quota for the same is not requested/updated. This results
in a revenue hole for prepaid subscribers.

For operators who have Stateful Firewall in-line service enabled, and are okay if packets are dropped, a
workaround is to configure the `firewall mime-flood` command in the ACS Configuration Mode, which enables
to configure the maximum number of headers allowed in an HTTP packet and the maximum header field size
allowed in the HTTP header (in bytes). However, a limitation of this workaround is that Stateful Firewall
supports MIME flood detection only in the downlink direction.

The support for LF termination has been added in StarOS 14.0 and later releases. For this release, with the
help of configurable maximum header length support, HTTP analyzer would be allowing such LF terminated
HTTP request/responses to pass through without rule matching only until the configured maximum header
length is reached. When this threshold is reached, immediately the analyzer marks such HTTP session as
failure and rule match would occur for `http error = TRUE` for the current packet as well as for all the previous
packets that passed through unmatched. At this point, the quota for all such packets will be requested and
reported.

Examples

The following command sets the HTTP header parse limit to 10000 bytes:

```
http header-parse-limit 10000
```
**ip reassembly-timeout**

This command allows you to configure how long to hold onto IP fragments for reassembly, while waiting for the complete packet to arrive.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

`[local] host_name(config-rule-base)#`

**Syntax Description**

`ip reassembly-timeout timeout_duration`

- **timeout_duration**

  Specifies the timeout duration, in milliseconds, to hold fragmented packets before reassembly. `timeout_duration` must be an integer from 100 through 30000.

**Usage Guidelines**

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.

**Examples**

The following command sets the timeout timer to 15000 milliseconds:

`ip reassembly-timeout 15000`
ip reset-tos

This command allows you to reset the IP Type of Service (ToS) value of incoming packets to the default QCI value, before proceeding with the rest of ACS processing.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

*active-charging service service_name > rulebase rulebase_name*

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

**Syntax Description**

| default | no | ip reset-tos |

**default**

Configures this command with its default setting.

Default: Disabled

**no**

If previously configured, deletes the IP reset-tos configuration from the current rulebase.

**Usage Guidelines**

Use this command to reset the ToS field of any packet after it reaches ACS, or to broaden the range of values that are used in the ToS field in the IP header of any packet.
**nat binding-record**

This command allows you to configure NAT Binding Record (NBR) generation.

---

**Important**

This command is only available in StarOS 8.3. In StarOS 9.0 and later releases this command is available in the Firewall-and-NAT Policy Configuration Mode.

---

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

**active-charging service** service_name > **rulebase** rulebase_name

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

```
nat binding-record edr-format edr_format_name | port-chunk-allocation | | port-chunk-release | +
{ default | no } nat binding-record
```

- **default**
  
  Configures this command with its default setting.
  
  Default: **port-chunk-release**

- **no**
  
  If previously configured, deletes the configuration from the current rulebase.

  **edr-format edr_format_name**

  Specifies the EDR format.

  *edr_format_name* must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.

  **port-chunk-allocation**

  Specifies generating NBR when a port chunk is allocated.
port-chunk-release
Specifies generating NBR when a port chunk is released.

+
Indicates that more than one of the previous keywords can be entered within a single command.

Usage Guidelines
Use this command to configure NBR generation.

Examples
The following command configures an EDR format named test123 and specifies generating NBR 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 allows you to enable/disable Network Address Translation (NAT) processing for all subscribers using the current rulebase.

---

**Important**

In StarOS 8.1 and StarOS 9.0 and later releases, 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, Stateful Firewall must be enabled for the subscriber. See the firewall policy CLI command.

---

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

**Syntax Description**

`nat policy nat-required [default-nat-realm nat_realm_name ]
{ default | no } nat policy`

**default**

Configures this command with its default setting.

Default: NAT processing is disabled for all subscribers using the current rulebase.

**no**

If previously enabled, disables NAT processing for all subscribers using the current rulebase.

**nat policy nat-required**

Enables NAT processing for all subscribers using the current rulebase.
default-nat-realm \texttt{nat\_realm\_name}

\textbf{Important} This keyword is only available in StarOS 8.3 and later releases.

Specifies the default NAT realm to be used if one is not already configured. 
\texttt{nat\_realm\_name} must be the name of a NAT realm, and must be an alphanumeric string of 1 through 31 characters.

\textbf{Important} Including the default NAT realm, a maximum of three NAT realms are supported.

\textbf{Usage Guidelines} Use this command to enable/disable NAT processing for all subscribers using the current rulebase.

After 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 \texttt{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.

\textbf{Examples} The following command enables NAT processing:
\texttt{n\at\ p\olicy\ n\at\-r\e\q\u\i\\r\e\i\\d\}}

The following command disables NAT processing:
\texttt{no n\at\ p\olicy}
nat suppress-aaa-update call-termination

This command allows you to suppress sending NAT Bind Updates (NBU) to the AAA server when a call gets terminated.

Important
This command is customer-specific. For more information please contact your Cisco account representative. In release 9.0, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product
NAT

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Rulebase Configuration
active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-rule-base)#

Syntax Description
nat suppress-aaa-update call-termination
default nat suppress-aaa-update

default

Configures this command with its default setting.
Default: Disabled. No suppression of AAA updates.

Usage Guidelines
Use this command to suppress the sending of NAT Bind Updates (NBU) to the AAA server when the call gets terminated, 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, NBUs are sent to the AAA server whenever a port chunk is allocated, de-allocated, or the call is cleared (PPP disconnect).

Examples

The following command suppresses the sending of NBU to the AAA server when PPP disconnect happens:
nat suppress-aaa-update call-termination
**override-control**

This command enables or disables Override Control (OC) feature. The Diameter capability exchange message should indicate support for OC feature when this CLI command is enabled.

---

**Important**

Override Control is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

---

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax Description**

```
[ default | no ] override-control [ with-oc-name ]
```

**default**

Configures this command with its default setting.

Default: Disabled

In 20 and later releases: If *with-oc-name* option is not configured in rulebase, OC will be identified using the Rule/CA and exclude rule as keys. This is the default behavior.

**no**

If previously enabled, disables Override control in the current rulebase.

**with-oc-name**

This optional keyword specifies to use OC-name as the unique key to identify an OC for a subscriber session.

Default: Disabled

In releases prior to 20, PCRF uses a combination of the following key parameters for identification of OC.

- Rule names
• Charging-action names
• Exclude-rule names

There is no unique OC name or ID to identify the OC for a particular subscriber session. In release 20, a new Diameter AVP "Override-Control-Name" is defined in the Override-Control grouped AVP. This OC name is used as the unique key to identify OC for any further updates like OC modification or deletion.

This keyword "with-oc-name" is added to the override-control CLI command to support Override-Control-Name AVP in the Override-Control AVP. If the override-control with-oc-name CLI is configured in rulebase, only OCs with Override-Control-Name AVP are supported and the OCs without name AVP are rejected.

If Override-Control-Name AVP is received when the override-control CLI command is configured, i.e. OC install is supported without OC name, appropriate error is reported in error logs. Then OC is dropped and OC failure statistics is incremented. Similarly if override-control with-oc-name CLI is configured and OC is received without the name AVP, appropriate error is reported, OC is dropped and OC failure statistics is incremented. On receiving an OC with-oc-name OC, installed OC list (without name) is searched for secondary identification criteria. If no OC with same rule/charging-action/exclude rule list is found, it is installed as a different OC.

Also, for OCs with the name AVP, operator can add rule/charging-action/exclude rule to the existing OC in the same category. That means, the rules can be added to a rule level OC, CA names can be added to a CA level OC, and exclude rules can be added to a wildcard or CA level OC.

OCs received with Override-Control-Name AVP are uniquely identified by the OC name. When the Override-Control-Name AVP is not present in Override-Control AVP, the OCs are identified based on the secondary identification criteria, i.e., the list of rule names, charging-action names, and exclude-rule names as these were the criteria before this feature change.

During rulebase change, the feature to support OC name will be controlled based on the configuration of new rulebase. After rulebase change OC will be accepted as per the CLI configured in new rulebase. This is the only scenario where for a single call session, OC can be installed with both OC name and without OC name.

When software upgrade is done on a standby setup where same rulebase is configured with the CLI override-control with-oc-name, then no calls are dropped and OC installation status will remain the same as before upgrade. Any new call which is established after upgrade and OC is installed with-oc-name then this will be accepted and applied on new call. Any calls which were established pre-upgrade will accept OC without name and will be identified uniquely by rule/charging-action/exclude rule.

During the downgrade, OC-name will be dropped and OCs will be recreated assuming Rule/CA/Exclude rule name list as the primary key for unique identification.

**Usage Guidelines**

Use this command to enable or disable Override Control feature and also specify to use Rule/CA list as unique key to identify OC for a session. This feature is available at the rulebase level and is license controlled. The Diameter capability exchange message should indicate support for Override control feature when this CLI command is enabled.

Inheritance feature does not support overwriting parameters at Rule level and charging action level and supports exclusion of only one rule. In order to provide this flexibility and also have a generic capability on chassis, Override Control feature is introduced. This feature will define a set of custom AVPs that will enable the PCRF to override charging and policy parameters for all rules (wildcard) or a specified set of rules or charging actions.

The override values should be sent by PCRF over Gx using the custom AVPs. Override Control provides this capability while addressing the limitations with Inheritance feature like rule level control, charging action.
level control, exclusion of more than one rule, different override values to be specified for a subscriber, etc. So, the Override Control feature will replace the Inheritance feature.

**Important**

In this release, both Inheritance and the Override Control features will be supported. Note that both these two features should not be enabled simultaneously. If by mistake, both these features are enabled, only Override Control is applied.

The Gx interface is updated to include custom AVPs for the PCRF to send override values to P-GW. These override values may be sent for all rules (wildcard) or for specific rule(s) or for charging action(s). In case the override values are sent for a charging action, a rule or some of the rules may be excluded from using the override values by sending the rules names in the Gx message. The override values will be check pointed and recovered in case of either standalone recovery or ICSR.

This Override Control feature is expected to maintain existing active calls using inheritance post upgrade. Inheritance feature and Override control should not be enabled simultaneously. It is necessary that Inheritance feature be turned off once Override Control feature is enabled. Override Control once enabled will apply only to new calls and does not effect existing calls.

Override Control feature allows the customer to dynamically modify the parameters of static or predefined rules with parameters sent by PCRF over the Gx interface.

When multiple overrides are received from PCRF, the following is the priority in which they are applied:

- Rule level override control
- Charging action level override control
- Wildcard level override control

When installing a predef rule, if override control is received for that predef rule and QCI/ARP is overridden, then the new overridden QCI/ARP values are used for bearer binding of the predef rule. If the QCI/ARP is not overridden, then the values configured in charging action is used. The override charging and policy parameters received from PCRF will continue to apply for the entire duration of the call. These values may be modified by PCRF by sending the modified values with the same override control criteria (Rule name(s), Charging Action Name(s) and Exclude Rule(s)). Any change in the Override Control criteria will be interrupted as a new OC. There can only be one wildcard OC installed for a subscriber.
p2p dynamic-flow-detection

This command allows you to enable/disable the P2P analyzer to detect peer-to-peer (P2P) applications.

**Product**
ADC

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**
<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
<th>p2p dynamic-flow-detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configures this command with its default setting.
Default: Disabled

| no |
If previously enabled, disables P2P dynamic flow detection in the current rulebase.

| p2p dynamic-flow-detection |
Enables dynamic P2P flow detection.

**Usage Guidelines**
Use this command to enable dynamic-flow detection. This allows the P2P analyzer to detect the P2P applications configured for the ACS.
pcp service

This command allows you to configure the PCP service for the current rulebase.

Important

This command is customer specific. Contact your Cisco account representative for more information.

Product

NAT
PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax Description

pcp service pcp_service_name
no pcp service

no

If previously configured, deletes the PCP service configuration from the current rulebase. This service is disabled by default.

pcp_service_name

Specifies the PCP service name for the current rulebase.

pcp_service_name must be the name of a PCP service, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure the PCP service for the current rulebase.

Examples

The following command configures a PCP service named pcp1 for the rulebase:

pcp service pcp1
**post-processing dynamic**

This command allows you to specify ruledefs/group-of-ruledefs as dynamic post-processing ruledefs/group-of-ruledefs. This allows the system to differentiate normal post-processing rules from preconfigured ones. By default, this configuration is disabled.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**

```
post-processing dynamic { group-of-ruledefs ruledefs_group_name | ruledef ruledef_name } charging-action charging_action_name [ description description ]
no post-processing dynamic { group-of-ruledefs ruledefs_group_name | ruledef ruledef_name }
```

**no**

If previously configured, deletes the specified configuration from the current rulebase.

**group-of-ruledefs ruledefs_group_name**

Adds the specified group-of-ruledefs to the current rulebase.

*ruledefs_group_name* must be the name of a group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.

**ruledef ruledef_name**

Adds the specified ruledef to the current rulebase.

*ruledef_name* must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

**charging-action charging_action_name**

Specifies the charging action.

*charging_action_name* must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.
description description
Specifies an optional description for this configuration.
description must be an alphanumerical string of 1 through 31 characters.

Usage Guidelines
Use this command to configure specific ruledefs/group-of-ruledefs as dynamic post-processing ruledefs/group-of-ruledefs. This allows the system to differentiate normal post-processing rules from the preconfigured ones. This makes possible enabling/disabling ruledefs/groups-of-ruledefs entry from an external server.

Examples
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
post-processing policy

This command allows you to specify the post-processing policy to be applied on Limit-Reached packets.

**Product**
- GGSN
- PDSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-rule-base) #
```

**Syntax Description**

```
post-processing policy { always | not-for-dynamic-discard }
default post-processing policy
```

**default**
Configures this command with its default setting.
Default: not-for-dynamic-discard

**always**
Specifies to apply post-processing even if the Credit Control Application (CCA) decides to discard packets due to limit-reached condition. If there are post-processing priority-based rules, CCA will check for any redirection rules. Otherwise, by default, CCA will discard the packets. No other post-processing actions like forward, next-hop, or xheader-insertion will be applied on the limit-reached packets.

**not-for-dynamic-discard**
Specifies to apply post-processing only if CCA decides not to discard packet. Will directly discard the limit-reached context and will not apply post-processing priority based rules.

**Usage Guidelines**
This command allows to enable post-processing priority based rules for content in blacklisted state. Whenever RADIUS/Diameter prepay server blacklists content the packets are generally discarded. To enable redirection
of such content, post-processing should be enabled on the blacklisted content. With this command, RADIUS/Diameter Credit-Control application will decide whether to allow post-processing to be enabled or not for the blacklisted content.

The following is a sample configuration:

```
configure
  active-charging service service1
  ruledef http_low
    http any-match = TRUE
    cca quota-state = limit-reached
    rule-application post-processing
    #exit
  ruledef http any
    http any-match = TRUE
    #exit
  charging-action standard1
    content-id 1
    cca charging credit
    #exit
  charging-action redirect
    flow action redirect-url http://aoc.com
    #exit
rulebase base1
  action priority 30 ruledef http any charging-action standard1
  post-processing policy always
  post-processing priority 1 ruledef http_low charging-action redirect
  #exit
end
```

**Examples**

The following command will enable post processing on Limit-Reached packets:

```
post-processing policy always
```
post-processing priority

This command allows you to configure the post-processing priority and action to be taken on specific ruledef in the current rulebase.

Important
This command is only available in StarOS 8.3 and later releases.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

(config-rule-base)#

Syntax Description

description

nopost-processingpriority

post-processing priority priority {group-of-rules ruledefs_group_name | ruledef ruledef_name }

charging-action charging_action_name | description description |

no

If previously configured, deletes the specified post-processing priority configuration from the current rulebase.

priority priority

Specifies priority for the ruledef/group-of-ruledefs in the current rulebase.

priority must be a unique value in the current rulebase, and must be an integer from 1 through 65535.

group-of-ruledefs ruledefs_group_name

Specifies the group-of-ruledefs.

ruledefs_group_name must be the name of a group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.
The group-of-ruledefs specified must be configured for post-processing. See the group-of-ruledefs-application command in the ACS Group-of-Ruledefs Configuration mode.

**Important**

ruledef **ruledef_name**

Specifies the ruledef.

`ruledef_name` must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

**Important**

The ruledef specified must be configured for post-processing. See the rule-application command in the ACS Ruledef Configuration Mode Commands chapter.

charging-action **charging_action_name**

Specifies the charging action.

`charging_action_name` must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

description **description**

Specifies an optional description for this configuration.

`description` must be an alphanumeric string of 1 through 31 characters.

**Usage Guidelines**

Use this command to configure the post-processing priority and action to be taken on a ruledef in the rulebase.

**Examples**

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`
qos-renegotiate timeout

This command allows you to configure the timeout setting for the Quality of Service (QoS) Renegotiation feature.

Important
This command is license dependent. For more information contact your Cisco account representative.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-rule-base)#

Syntax Description
qos-renegotiate timeout timeout
no qos-renegotiate timeout

no
If previously configured, deletes the qos-renegotiate timeout configuration from the current rulebase.

timeout
Specifies the timeout period for the QoS Renegotiation feature in the current rulebase.

timeout is the timeout period in seconds, and must be an integer from 0 through 4294967295. If set to 0, timeout is disabled.

Usage Guidelines
Use this command to configure timeout setting for the QoS Renegotiation feature.

Examples
The following command sets the QoS renegotiate timeout period to 1000 seconds:
qos-renegotiate timeout 1000
radius threshold

This command allows you to configure the interval and volume thresholds to generate interim RADIUS Charging Data Records (CDRs) and write them to CDR file for ACS postpaid billing.

Product

HA
PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration
active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:
[local] host_name (config-rule-base) #

Syntax Description

radius threshold { interval interval | volume total volume }
{ default | no } radius threshold { interval | volume total }

no
If previously configured, deletes the RADIUS threshold configuration from the current rulebase.

default
Configures this command with the default settings.
Default: Disabled

interval interval
Specifies the time interval, in seconds, for generating RADIUS interim accounting requests.
interval must be an integer from 60 through 40000000.
Default: Disabled

volume total volume
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 100000 through 4000000000.
Default: Disabled
**Usage Guidelines**

Use this command to specify a time interval threshold to generate interim RADIUS CDRs and write it to RADIUS CDR file for postpaid billing.

**Examples**

The following command configures a time threshold interval of 600 seconds for RADIUS CDRs:

```
radius threshold interval 600
```
retransmissions-counted

This command allows to count retransmissions in all charging modules.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax Description
[ no ] retransmissions-counted

no
Retransmissions will be counted for all the charging modules. This command will override the CLI at the charging action as well as the CLI pertaining to the retransmissions at the rulebase.

Usage Guidelines
Use this command to count retransmissions for all the charging modules.

Examples
With the following command, retransmissions will not be counted for any of the charging modules:

no retransmissions-counted
**ran bandwidth optimize**

This command is used to enable optimized calculation of [MBR, GBR] when a subscriber (voice) call is put on hold in case of VoLTE.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

**active-charging service service_name > rulebase rulebase_name**

Entering the above command sequence results in the following prompt:

[local] host_name(config-rule-base)#

**Syntax Description**

| default | no | ran-bandwidth optimize |

**no**

If previously configured, disables the optimization feature for calculating [MBR, GBR] values based on Flow-Status AVP value.

**Usage Guidelines**

Use this command to enable optimized calculation of [MBR, GBR] values when a subscriber (voice) call is put on hold in case of VoLTE.

When the rule is installed and active, the system uses the GBR/MBR assigned in the rule for calculating the GBR/MBR values towards the bearers created. When more than one rule is installed, P-GW adds the GBR/MBR values from all the active and installed rules even if the flow of a certain rule is marked as disabled. This current behavior is in accordance with 3GPP TS standard specification 29.212, and this might result in RAN bandwidth wastage. To avoid this wastage, some optimization is done while calculating MBR and GBR for GBR bearer.

This optimization feature provides the ability to configure a list of APNs, for which the optimized calculation of MBR, GBR can be enabled. By default, this optimized calculation should be enabled only for the IMS APN.

This feature further helps optimize the logic of aggregating MBR and GBR values, based on "Flow-Status" AVP value received in the rule definition through RAR.

During session setup, when a CCA-I is received, and if ran bandwidth optimize is configured for the associated rulebase, the system will aggregate [MBR, GBR] of only the rules which have flow-status="ENABLED". This information will subsequently be sent to UE.
Important

The last used [MBR, GBR] for GBR bearer needs to be recovered in the event of a session manager or chassis switchover. Failure to do so can result in miscalculation of [MBR, GBR] after recovery.

By default, this CLI will be disabled. Any change in this configuration will not affect existing calls on the system. Optimized bandwidth calculation will be done only for the new calls established after enabling this CLI command.
route priority

This command allows you to configure the routing of packets to protocol analyzers.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

**Syntax Description**

```plaintext
route priority route_priority ruledef ruledef_name analyzer { dns | file-transfer | ftp-control | ftp-data | h323 | http | imap | mipv6 | mms | pop3 | pptp | radius | rtp | rtsp | sdp | secure-http | sip | advanced | basic-and-advanced | smtp | tftp | wsp-connection-less | wsp-connection-oriented } [ description description ]
no route priority route_priority
```

**no**

If previously configured, deletes the specified route priority configuration from the current rulebase.

**route priority route_priority**

Specifies the route priority for the specified 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 analyzer.

`ruledef_name` specifies the name of the ruledef configured for the route application using the `rule-application` command in the ACS Ruledef Configuration Mode.

`ruledef_name` must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

**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.

• **h323**: Route to H323 protocol analyzer.

• **http**: Route to HTTP protocol analyzer.

• **imap**: Route to IMAP protocol analyzer.

• **mipv6**: Route to MIPv6 protocol analyzer.

• **mms**: Route to MMS protocol analyzer.

• **pop3**: Route to POP3 protocol analyzer.

• **pptp**: Route to PPTP protocol analyzer.

• **radius**: Route to RADIUS protocol analyzer.

• **rtcp**: Route to RTCP protocol analyzer.

• **rtp**: Route to RTP protocol analyzer.

• **rtsp**: Route to RTSP protocol analyzer.

• **sdp**: Route to SDP protocol analyzer.

• **secure-http**: Route to secure HTTP protocol analyzer.

• **sip [advanced | basic-and-advanced]**: Route to SIP protocol analyzer.
  
  • **advanced**: For SIP calls to work with NAT/Stateful Firewall, a SIP Application-Level Gateway (ALG) is required to do payload translation of SIP packets and pin-hole (dynamic flow) creation for media packets. A SIP routing rule must be configured for routing the packets to the SIP ALG for processing. If the keyword **advanced** is configured, the packets matching the routing rule will be routed to SIP ALG for processing and not to ACS SIP analyzer. If not configured, then packets will not be routed to SIP ALG and will be routed to ACS SIP analyzer for processing.

  Also, see **firewall nat-alg** CLI command in the ACS Configuration Mode.

  • **basic-and-advanced**: For SIP ALG to co-exist with SIP Analyzer, the packets are routed through ACS SIP Analyzer and SIP ALG. The SIP packets can pass through ACS functionality (by ACS SIP Analyzer processing) and at the same time payload translation/pinhole-creation can happen successfully (by SIP ALG processing). If **basic-and-advanced** is configured, then the packets matching the routing rule will be routed through the SIP Analyzer and then through SIP ALG for processing.

• **tftp**: Route to TFTP protocol analyzer.

• **smtp**: Route to SMTP protocol analyzer.

• **wsp-connection-less**: Route to WSP connection-less protocol analyzer.

• **wsp-connection-oriented**: Route to WSP connection-oriented protocol analyzer.
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.

Use the `show active-charging analyzer statistics` command in the Exec Mode to see the list of supported analyzers.

description

Enables to add a description to the rule and action for later reference in saved configuration file. `description` must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Instances of this CLI command control which packets are routed to which protocol analyzers. Packets sent to ACS 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>dns</td>
<td>UDP destination port or source port is DNS (53).</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>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>http</td>
<td>TCP destination port or source port is HTTP (80).</td>
</tr>
<tr>
<td>icmp</td>
<td>All IPv4 packets with IP protocol = ICMP (1) are automatically routed here.</td>
</tr>
<tr>
<td>imap</td>
<td>TCP destination port or source port is IMAP (143).</td>
</tr>
<tr>
<td>ip</td>
<td>All IPv4 packets are automatically routed here.</td>
</tr>
<tr>
<td>mipv6</td>
<td>MIPv6 analyser can be routed in one of the following ways:</td>
</tr>
<tr>
<td></td>
<td>• All IPv4 UDP packets with destination port = 5846</td>
</tr>
<tr>
<td></td>
<td>• All IPv4 UDP packets with destination port = 5846, and destination IP present in LMA server host-pool</td>
</tr>
<tr>
<td></td>
<td>• All IPv6 packets with destination IP present in LMA server host-pool</td>
</tr>
<tr>
<td>mms</td>
<td>WSP content type is application/vnd.wap.mms-message; or, WSP uri contains &quot;mms&quot;; or, HTTP content type is application/vnd.wap.mms-message; or, HTTP uri contains &quot;mms&quot;.</td>
</tr>
<tr>
<td>Analyzer</td>
<td>Common ways to route to the analyzer</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------</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>
<tr>
<td>pop3</td>
<td>TCP destination port or source port is POP3 (110).</td>
</tr>
<tr>
<td>radius</td>
<td>UDP source or destination port 1812 to be used.</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>sdp</td>
<td>RTSP or SIP content type is application/sdp</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>sip</td>
<td>UDP destination port or source port is SIP (5060).</td>
</tr>
<tr>
<td>smtp</td>
<td>TCP destination port or source port is SMTP (25).</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>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 <strong>wap</strong> analyzer if the carrier does not use a special port number.</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 &quot;wsp-connection-oriented&quot; as described above.</td>
</tr>
</tbody>
</table>
route priority

Examples

The following command assigns a route and rule action with the route priority of 23, a ruledef named 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 allows you to enable/disable the Real Time Streaming Protocol (RTSP) and Session Description Protocol (SDP) analyzers to detect the start/stop of RTP and RTCP flows.

Product  ACS

Privilege  Security Administrator, Administrator

Command Modes  Exec > ACS Configuration > Rulebase Configuration

    active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

    [local]host_name(config-rule-base)#

Syntax Description  \[ default | no \] rtp dynamic-flow-detection

    default
    Configures this command with its default setting.
    Default: Disabled; same as no rtp dynamic-flow-detection.

    no
    If previously configured, deletes this configuration from the current rulebase.

Usage Guidelines  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.

Examples  The following command enables RTP dynamic flow detection:

    rtp dynamic-flow-detection
rtsp initial-bytes-limit

This command allows to set the maximum number of uplink and downlink bytes, added together to accumulate, while rule matching and charging is being delayed for RTSP flows. The limit is per RTSP flow.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Rulebase Configuration

active-chargingservice service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax Description
rtsp initial-bytes-limit rtsp_bytes
default rtsp initial-bytes-limit

default
Configures the RTSP initial packets limit to 6000 bytes.

RTSP_bytes
Specifies the maximum number of uplink and downlink bytes limit.
rtsp_bytes must be an integer from 1 through 256000.

Usage Guidelines
Use this command to configure the maximum number of uplink and downlink bytes per RTSP flow that can be accumulated before the first SETUP request. The accumulated bytes include both TCP-control packets as well as RTSP packets. Once this limit is reached, rule matching occurs and charging is enforced on the flow. This command is used in conjunction with the flow rtsp-all-pkts charge-to-application command.

Examples
The following command sets the RTSP initial bytes limit to 9000 bytes:
rtsp initial-bytes-limit 9000
ruledef-parsing

This command allows you to configure whether to consider or ignore the port number embedded in the application header (for example, the ":80" in www.star.com:80) when comparing the ruledef expressions to the packet contents.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base) #
```

**Syntax Description**

```
[ no ] ruledef-parsing ignore-port-numbers-embedded-in-application-headers analyzers { http rtsp sip wsp }
default ruledef-parsing
```

```
no
```

If previously configured, deletes the ruledef-parsing configuration from the current rulebase.

```
default
```

Configures this command with its default setting.

Default: Same as 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 }
```

Ignore the port numbers present in application header.

Specifies analyzers for which the port number must be ignored.

**Usage Guidelines**

Use this command to make the HTTP, RTSP, SIP, and WSP analyzer ignore port numbers embedded in application headers.
Examples

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 allows you to configure how long to retain the TCP flow after the FIN has been acknowledged.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-rule-base) #

**Syntax Description**

tcp 2msl-timeout 2msl_timeout [ port-reuse ]

{ default | no } tcp 2msl-timeout

default

Configures this command with its default setting.

Default: 2 seconds

no

Disables the timeout and sets the system to delete the flow immediately upon seeing the FIN acknowledged.

**Usage Guidelines**

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.
The following command sets the timeout to 4 seconds:

```
tcp 2msl-timeout 4 port-reuse
```
tcp check-window-size

This command allows you to enable/disable TCP window-size checking.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration
active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-rule-base)#

**Syntax Description**
[ default | no ] tcp check-window-size

- **default**
  Configures this command with its default setting.
  Default: Enabled (packets after the erroneous packet (with size greater than the receiver's window size) will hit tcp-error ruledef).

- **no**
  Disables the window-size check and continues with normal L7 parsing.

- **tcp check-window-size**
  Enables the window-size check and continues with normal L7 parsing.

**Usage Guidelines**
Use this command to enable/disable TCP window-size check for packets out of TCP window.

**Examples**
The following command enables TCP window-size check:

```
tcp check-window-size
```
**tcp mss**

This command allows you to configure the TCP Maximum Segment Size (MSS) in TCP SYN packets.

This command is only available in StarOS 8.1 and later releases.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-rule-base)#
```

**Syntax Description**

```
tcp mss tcp_mss { add-if-not-present | limit-if-present } +
{ default | no } tcp mss
```

**default**

Configures this command with its default setting.
Default: Disabled

**no**

If previously configured, deletes the TCP MSS configuration from the current rulebase.

**tcp mss tcp_mss**

Specifies the TCP MSS.
	`tcp_mss` must be an integer from 496 through 65535.

**add-if-not-present**

Specifies to add the TCP MSS if not present in the packet.

**limit-if-present**

Specifies to limit the TCP MSS if present in the packet.
Usage Guidelines

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 memory 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.

Examples

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 allows you to configure processing of TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax Description tcp packets-out-of-order { timeout timeout_duration | transmit | after-reordering | immediately }
default tcp packets-out-of-order { timeout | transmit }

default
Configures this command with its default setting.

- **timeout**: 5000 milliseconds
- **transmit**: immediately

**timeout timeout_duration**

 Specifies the timeout duration for re-assembly of TCP out-of-order packets.

*timeout_duration* is the timeout duration, in milliseconds, and must be an integer from 100 through 30000. Default: 5000 milliseconds

**transmit | after-reordering | immediately**

Configures the TCP out-of-order segment behavior after buffering a copy.

- **after-reordering**: Delivers the TCP out-of-order segments in-sequence to the ECS analyzer after all packets are received and successfully reordered. The 'after-reordering' feature is doing this by buffering out-of-order packets, and only releasing them after the missing out-of-order packets are received (or after OOO timeout).
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 (as the latest). If reordering is not successful within the specified OOO timeout, all the subsequent received packets in that TCP flow are forwarded without being passed through the analysers (except the L3/L4 analyzer). As a consequence only L3/L4 rule matching will take place. If memory allocation fails or the received packet is partial retransmitted data, the packet will also be forwarded immediately without being passed through the protocol analyzers, except for the L3/L4 analyzers.

**Important**

On the outgoing interface, no in-sequence delivery is guaranteed. This feature is intended to:
- deliver the TCP segments in-order to the ECS analysers
- buffer the original packets during OOO conditions, such that application-based flow actions (ex: Header insertion) can still take place on the actual data packets
- Its not intended to put the packets in-sequence on the outgoing interface (although some improvement can be seen there as well)
- the cost of this feature is additional delay for OOO packets (up to a maximum of the OOO timeout).

- **Immediately**: Delivers the TCP out-of-order segments in-sequence to the ECS analyzer after all packets are received and successfully reordered. The 'immediately' feature is accomplishing this by making a copy of out-of-order packets, and buffering those, while transmitting the original data packets through the outgoing interface immediately. 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.

  If reordering of the buffered packets is not successful within the specified OOO timeout, all the subsequent received packets in that TCP flow are forwarded without being passed through the analysers (except the L3/L4 analyzer). As a consequence only L3/L4 rule matching will take place.

  If memory allocation fails or the received packet is partial retransmitted data, the packet will also be forwarded immediately without being passed through the protocol analyzers, except for the L3/L4 analyzers.

**Important**

This feature is not changing anything on the sequencing of the packets. This feature has the consequence that during OOO conditions, certain application-based flow actions (ex: Header insertion) could not take place as the original packets are already sent out by the time the ECS analyzer receives the (copies of) in-sequence packets.

Default: **immediately**

**Usage Guidelines**

Use this command to configure how to process TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

**Important**

When TCP OOO processing has been configured in the rulebase, a session manager crash might be observed due to overlapping TCP segments and/or reordering packet arriving within TCP OOO configured timeout value or default value (5 sec). This issue can be resolved by changing the rulebase configuration for TCP OOO packets from **transmit after-reordering** to **transmit immediately**.
Examples

The following command sets the timeout timer to 10000 milliseconds:

tcp packets-out-of-order timeout 10000
tcp proxy-mode

This command allows you to enable/disable TCP Proxy mode for all subscribers using the current rulebase.

**Important**

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product**

ACS
CF
MVG
TPO

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-rule-base)#

**Syntax Description**

tcp proxy-mode { dynamic { all | content-filtering | dcca | ip-readdressing | nexthop-readdressing | xheader-insert } + | static { port { port_number | to port_number } | | } }

default tcp proxy-mode

no tcp proxy-mode { dynamic { content-filtering | dcca | ip-readdressing | nexthop-readdressing | xheader-insert } + | static { port { port_number | to port_number } | | } }

**default**

Configures this command with its default setting.
Default: Disabled

**no**

If previously enabled, disables TCP Proxy mode.
Optionally, TCP Proxy can be disabled for specific options that were previously enabled.
**Dynamic TCP Proxy Mode**

```plaintext
dynamic { all | content-filtering | dcca | ip-readdressing | nexthop-readdressing | xheader-insert } +
```

Enables TCP proxy for subscriber-initiated TCP flows under the specified condition(s).

- **all**: Specifies that subscriber-initiated TCP flows be proxied if all/any of the following conditions are satisfied.
- **content-filtering**: Specifies that subscriber-initiated TCP flows be proxied if a URL is requested, and that URL is checked because Category-based Content Filtering is enabled in the rulebase.
- **dcca**: Specifies that subscriber-initiated TCP flows be proxied if DCCA is enabled in the charging action.
- **ip-readdressing**: Specifies that subscriber-initiated TCP flows be proxied if IP Readdressing feature is enabled in the charging action.
- **nexthop-readdressing**: Specifies that subscriber-initiated TCP flows be proxied if Nexthop Readdressing feature is enabled in the charging action.
- **xheader-insert**: Specifies that subscriber-initiated TCP flows be proxied if x-Header Insertion feature is enabled in the charging action.

**Static TCP Proxy Mode**

```plaintext
static [port {port_number [to port_number]}]
```

Enables static TCP proxy for every subscriber-initiated TCP flow, unless specific ports are specified.

```plaintext
port {port_number [to port_number]}
```

Specifies port numbers and/or range of port numbers.

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

---

**Important**

Up to 32 port numbers and eight port ranges can be specified.

---

**Usage Guidelines**

- **Important**: In release 11.0, TCP Proxy functions only in Static mode. Dynamic TCP Proxy mode is supported only in 12.0 and later releases.

Use this command to enable/disable TCP Proxy mode for all subscribers using this ACS rulebase. Optionally, TCP Proxy can be enabled/disabled for specific ACS features. Note that enabling/disabling the TCP Proxy feature for any of the optional ACS features, does not affect that feature.

Note that the last command overwrites any previous configuration. For example, when the following commands are applied in sequence:

```plaintext
tcp proxy-mode dynamic nexthop-readdressing
tcp proxy-mode dynamic xheader-insert
```

The nexthop configuration is overwritten by the x-header configuration.

---

**Examples**

The following command enables TCP proxy for subscriber-initiated TCP flows whenever next-hop-forwarding-address is configured in the charging action:

```plaintext
tcp proxy-mode dynamic nexthop-readdressing
```
**tethering-detection**

This command allows you to enable/disable the Tethering Detection feature for the current rulebase, and specifies the database to use.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]\host_name(config-rule-base)#

**Syntax Description**

`tethering-detection [ip-ttl value ttl_value] [max-syn-packet-in-flow max_syn_packets] [os-db-only] [os-ua-db] [ua-db-only] {default|no} tethering-detection`

**default**

Configures this command with its default setting.

Default: By default, the Tethering Detection feature is disabled. When enabled, unless a specific database is specified to be used, by default tethering detection will make use of both the databases.

**no**

If previously configured, deletes the tethering detection configuration from the current rulebase.

**ip-ttl value ttl_value**

Specifies to perform tethering detection using IP-TTL configuration. `ttl_value` must be an integer from 1 through 255 to configure TTL values for tethered flows.

**max-syn-packet-in-flow max_syn_packets**

Specifies the number of SYN packets applicable for tethering detection in a flow. `max_syn_packets` must be an integer from 1 through 3.

Default number of SYN packets is 1. This means that only the first SYN packet in flow will be analyzed for IP-TTL/OS signature generation and tethering detection. All other mid-flow SYN packets will be ignored for IP-TTL/OS signature generation and tethering detection.
**os-db-only**
In 17 and earlier releases: Specifies to perform tethering detection using only the OS signature database.
In 18 and later releases: Specifies to perform tethering detection using IPv4 and IPv6 OS signature databases.

**os-ua-db**
In 17 and earlier releases: Specifies to perform tethering detection using only OS and UA signature databases.
In 18 and later releases: Specifies to perform tethering detection using IPv4 OS, IPv6 OS, and UA signature databases.

**ua-db-only**
Specifies to perform tethering detection using only the UA signature database.

**Usage Guidelines**
Use this command to enable/disable the Tethering Detection feature for a rulebase, and configure the database to use. Tethering Detection can be done for IPv4, IPv6, TCP and UDP flows.
Changing the configuration does not affect existing flows of the subscriber. If Tethering Detection was disabled and is turned enabled, it will be applied only to new flows of subscribers using the rulebase.

**Important**
IPv6 Tethering Detection is supported only with TTL and UA signatures, and not supported for OS signatures.

Also, see the `tethering-database` command in the *ACS Configuration Mode Commands* chapter.

**Examples**
The following command enables the Tethering Detection feature in the rulebase, and specifies to use only the OS database:

```
tethering-detection os-db-only
```
**tft-notify-ue-def-bearer**

This command allows you to control whether TFT updates are sent to UE or not for default bearer for the specified rulebase.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-rule-base) #
```

**Syntax Description**

```
{ default | no } tft-notify-ue-def-bearer
```

**default**

The default behavior is to send the TFT updates of default bearer for the specified APN to UE.

**no**

This keyword controls the TFT updates of default bearer for the APN attached to the chassis, from being sent to the UE.

**Usage Guidelines**

Use this command at the rulebase level to control whether TFT updates are sent to UE or not for default bearer for the specified rulebase.

This feature provides the operator the flexibility to configure this per Rulebase and also configure to suppress TFT updates only. The CLI command allows sending other QoS updates to the UE and controls only the TFT related updates. This CLI is supported only for default bearer.

In releases prior to 15.0, the "no policy-control update-default-bearer" CLI command is used to suppress all the TFT updates to the UE on the default bearer including the initial TFTs sent in the Create Session Response. Also, this configuration is available for the entire system and not per rulebase. Additionally, this CLI command suppresses all the QoS related updates (including change in bit rate) to the UE.
**timestamp rounding**

This command allows you to enable/disable timestamp rounding in EDRs or eG-CDRs.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-rule-base) #

**Syntax Description**

timestamp rounding { edr | egcdr } { ceiling | floor | round-off }

{ default | no } timestamp rounding { edr | egcdr }

**default**

Configures this command with its default setting.

Default: round-off

**no**

Disables timestamp rounding.

**edr**

Enables timestamp rounding for EDRs.

**egcdr**

Enables timestamp rounding for eG-CDRs.

**ceiling**

If the fractional part of the seconds is greater than 0, adds 1 to the number of seconds and discards the fraction.

**floor**

Discards the fractional part of the second.
round-off
Sets the fractional part of the seconds to nearest integer value. If the 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 Guidelines
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 (for example, 2 – 1 = 1). This command may be repeated for each type of EDR or eG-CDR.

Examples
The following command sets the EDR timestamp to nearest integer value second; for example, 34:12.23 to 34:12.00:

timestamp rounding edr round-off
tpo default-policy

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
**transactional-rule-matching**

This command allows you to enable or disable transactional rule matching (TRM) which allows the Enhanced Charging Service (ECS) to bypass per-packet rule matching on a transaction once the transaction is fully classified.

---

**Important**

The TRM feature is supported in SSI platform; earlier it was restricted only to ASR5500.

---

**Product**

ACS

ADC

**Privilege**

Security Administrator, Administrator

**Command Modes**

`Exec > ACS Configuration > Rulebase Configuration`

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-rule-base)#
```

**Syntax Description**

```
| default | no | transactional-rule-matching
```

**default**

Configures this command with its default setting.

Default: Disabled.

**no**

If already configured, disables transactional rule matching.

**Usage Guidelines**

Use this command to enable or disable transactional rule matching. This allows the Enhanced Charging Service (ECS) to bypass per-packet rule matching on a transaction once the transaction is fully classified.

A transaction for TRM can be defined as the entire UDP flow, the ACK of the 3-way handshake to the FIN/RST of a TCP flow, or the HTTP request to the next HTTP request, or HTTP request to the FIN/RST for the final request of the flow. Rule matching can be performed on IP L4 rules (UDP, TCP), HTTP, and HTTPS.
In 16.0 and later releases, ADC and TRM/FP can be enabled together. ADC flows will be considered for TRM optimization. Most VoIP applications that require all packets of the flow do not support TRM. When TRM/FP is enabled with ADC, such protocols will not take TRM/FP.

**Important**

From 16.0 release, **Transactional Rule Matching** and **Fastpath** functionalities have been merged, and will be governed by only the **transactional-rule-matching** keyword alone. The keyword **fastpath** independently can no longer be used to turn on or turn off this functionality.

**Examples**

The following command enables transactional rule matching:

```plaintext
transactional-rule-matching
```
transport-layer-checksum

This command allows you to enable/disable checksum verification for TCP and UDP packets.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax Description

| 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

Configures this command with its default setting.

Default: Same as 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/not verified.

If neither of these keywords is specified the command applies to both TCP and UDP packets.

Usage Guidelines

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 via the route 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).
Examples

The following command disables checksum verification calculations on all TCP and UDP packets:

```plaintext
transport-layer-checksum verify-during-packet-inspection
```

```plaintext
no transport-layer-checksum verify-during-packet-inspection
```
udr threshold

This command allows you to configure the threshold limit to generate Usage Data 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

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax Description

udr threshold { interval interval | volume { downlink bytes | uplink bytes | total bytes | downlink bytes | uplink bytes } }

default udr threshold { interval | volume }

no udr threshold { interval | volume { downlink | uplink | total | uplink | downlink } }

no

If previously configured, deletes the UDR threshold configuration from the current rulebase.

default

Configures this command with its default setting.

Default: Disabled; same as no udr threshold interval and no udr threshold volume.

interval interval

Specifies the time interval, in seconds, for closing the UDR if the minimum time duration thresholds are satisfied. By default, this option is disabled.

interval must be an integer from 60 through 40000000.

Default: 0 (Disabled)

volume

Specifies uplink/downlink volume octet counts for the generation of interim UDRs.
• **downlink bytes**: Specifies the limit for the number of downlink octets after which the UDR is closed. 
  *bytes* must be an integer from 100000 through 4000000000.
  Default: 4000000000

• **total bytes**: Specifies the limit for the total number of octets (uplink+downlink) after which the UDR is closed.
  *bytes* must be an integer from 100000 through 4000000000.
  Default: Disabled

• **uplink bytes**: Specifies the limit for the number of uplink octets after which the UDR is closed.
  *bytes* must be an integer from 100000 through 4000000000.
  Default: 4000000000

UDR records are generated whenever either threshold is reached.

**Usage Guidelines**

Use this command to enable thresholds for generation of UDRs.

**Examples**

The following command specifies that UDR records should be generated every 10 minutes (*600 seconds*):

```
udr threshold interval 600
```
udr trigger

This command allows you to configure additional triggers for generating UDRs.

Important

This command is only available in StarOS 8.3 and later releases.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-rule-base) #

Syntax Description

- `udr trigger { first-hit-content-id | tariff-time minute minutes hour hours | nemo-prefix-update }`
- `no udr trigger { first-hit-content-id | tariff-time | nemo-prefix-update }`
- `default udr trigger | nemo-prefix-update` | }
- `no`

Disables first-hit-content-id UDR trigger.

- `default`

Configures this command with its default setting.

Default: Disabled; no additional triggers.

- `first-hit-content-id`

Specifies to generate interim UDR on first packet hit per rating group/content ID.

- `tariff-time minute minutes hour hours`

This keyword allows to configure tariff time trigger to close ongoing UDR buckets and save all data traffic up to tariff time in a single UDR file. By default, this CLI keyword is disabled.

Configuring this keyword enables the PDSN/PCEF to generate content base UDR record for each concurrent online subscriber in each of day cross and place them in a single UDR file. The charging records include content based service (by duration and by volume).
Tariff time is stored at rulebase level. Therefore if the tariff time is updated while there are ongoing calls in the network, the old tariff time will be ignored and the new tariff time will be applied to the existing as well as upcoming calls.

At the end of the "Tariff Time" period, the UDR files are created and the next set of records are stored in a new UDR file.

**nemo-prefix-update**

<table>
<thead>
<tr>
<th>Important</th>
<th>This keyword is available only with NEMO license.</th>
</tr>
</thead>
</table>

On configuring this keyword/trigger, UDRs will be generated in case a NEMO update event is received. If this trigger is not configured UDRs will not be generated even if a NEMO update event is received from session manager. If the "no" or "default" option is used, it will disable the UDR trigger for nemo-prefix-update.

**Usage Guidelines**

This command enables to assign first packet trigger to interim UDRs—for generating UDR for first packet hit per rating group/content ID. The first-hit-content-id trigger when configured causes an UDR to be generated as soon as a packet hits a Charging Action with a content ID. UDR generation will be triggered when this command is configured and present in the rulebase.

**Examples**

The following command assigns first packet trigger to interim UDRs, for generating UDR for first packet hit per rating group/content ID:

```bash
udr trigger first-hit-content-id
```
url-blacklisting action

This command allows you to enable/disable URL Blacklisting functionality for the current rulebase, and configures the action to be taken when there is a URL match.

**Product**

CF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

**Syntax Description**

url-blacklisting action { discard | redirect-url url | terminate-flow | www-reply-code-and-terminate-flow reply_code } [ content-id content_id ]

{ default | no } url-blacklisting action

default

Disables URL Blacklisting in the current rulebase.

no

If previously configured, deletes the URL Blacklisting action configuration from the current rulebase.

discard

Configures URL Blacklisting "discard" action.

redirect-url url

Configures URL Blacklisting "redirect-url" action.

*url* specifies the redirect URL/URI, which must be a fully qualified URL/URI, and must be an alphanumeric string of 1 through 1023 characters.

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.

**content-id** `content_id`

Usage Guidelines

Use this command to enable/disable URL Blacklisting at the rulebase level, and configure the action to be taken.

Examples

The following command enables URL Blacklisting in the rulebase, 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 allows you to enable/disable a group-of-prefixed-urls for preprocessing of embedded URLs.

Important

This command is customer specific. For more information, please contact your Cisco account representative.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-rule-base) #

Syntax Description

| no | url-preprocessing bypass group-of-prefixed-urls prefixed_urls_group_name

no

If previously configured, deletes the URL-preprocessing bypass configuration from the current rulebase.

group-of-prefixed-urls prefixed_urls_group_name

Specifies the group-of-prefixed-urls.

prefixed_urls_group_name must be the name of a group-of-prefixed-urls, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to enable/disable a group-of-prefixed-urls for preprocessing of embedded URLs. This command can be issued multiple times to enable multiple groups. If an embedded URL begins with the string specified within any of the groups, that prefix text will be removed from the URL.

Examples

The following command enables looking for prefixed URLs of the group-of-prefixed-urls named test5:

url-preprocessing bypass group-of-prefixed-urls test5
**video optimization-preprocessing cae-readdressing**

This command allows you to enable/disable CAE readdressing at the rulebase level.

---

**Important**

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.</td>
</tr>
</tbody>
</table>

---

**Product**

ACS  
MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax Description**

```
video optimization-preprocessing cae-readdressing

[ default | no | video optimization-preprocessing

default

Configures this command with its default setting.

no

If already configured, disables CAE readdressing.
```

**Usage Guidelines**

Use this command to configure ACS to readdress the flows to CAE.
websocket flow-detection

This command allows you to enable or disable websocket flow detection at rulebase level.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Rulebase Configuration
active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-rule-base)#

Syntax Description
| no | websocket flow-detection | protocol1 | protocol2 | protocol3 | ... |

no
Disables the websocket flow detection.

| protocol1 | protocol2 | protocol3 | ... | Specifies protocol for detection.
If both protocol1 and protocol2 are specified, then specifies protocol detection of both protocols.

Usage Guidelines
Use this command to disable or enable websocket flow detection identification of protocols.

Important
Currently, websocket is only using HTTP protocol as a transport layer, so the CLI will have only http as option.

Examples
The following command disables websocket flow detection identification of protocols:
no websocket flow-detection [proto1 | proto2 | proto3 ]
**wtp out-of-order-timeout**

**Description** This command has been deprecated, and is replaced by the command.
wtp packets-out-of-order

This command allows you to configure how to process Wireless Transaction Protocol (WTP) packets that are out of order, while waiting for the earlier packet(s) to arrive.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax Description
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
Configures this command with its default setting.

  • out-of-order-timeout: 5000 milliseconds
  • transmit: immediately

out-of-order-timeout timeout
Specifies the maximum duration for which WTP out-of-order packets are retained, 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: Sends WTP out-of-order segment after it becomes ordered
  • immediately: Sends WTP out-of-order segment immediately after buffering a copy

Default: immediately
 Usage Guidelines

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).

 Examples

The following command sets the timeout timer to 10000 milliseconds:

```
  wtp packets-out-of-order out-of-order-timeout 10000
```
**xheader-encryption**

This command allows you to configure X-Header Encryption feature’s parameters.

---

**Important**

This command is license dependent. For more information please contact your Cisco account representative.

---

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Rulebase Configuration

active charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-rule-base) #

**Syntax Description**

```
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 this command with its default setting.
Default: Disabled

no
If previously configured, deletes the configuration from the current rulebase.

certificate-name certificate_name
Specifies the encryption certificate to use for the X-Header Encryption feature.

certificate_name must be the name of an encryption certificate, and must be an alphanumeric string of 1 through 63 characters.
Default: Disabled; no encryption certificate

re-encryption period 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. Default: Disabled; no re-encryption

**Usage Guidelines**
Use this command to configure the X-Header Encryption feature's certificate and re-encryption parameters.

**Examples**
The following command configures the X-Header Encryption feature to use the certificate named *testcert*:
```
xheader-encryption certificate-name testcert
```
xheader-encryption
ACS Ruledef Configuration Mode Commands

Important

In 14.1 and earlier releases, up to 10 rule expressions can be configured in one ruledef. In 15.0 and later releases, up to 32 rule expressions can be configured in one ruledef.

The ACS Ruledef Configuration Mode is used to create and manage rule expressions in individual rule definitions (ruledefs).

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Important

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

- bearer 3gpp apn, page 790
- bearer 3gpp imsi, page 792
- bearer 3gpp rat-type, page 794
- bearer 3gpp sgsn-address, page 796
- bearer 3gpp2 bsid, page 798
- bearer 3gpp2 service-option, page 800
- bearer apn, page 802
- bearer imsi, page 804
- bearer rat-type, page 806
- bearer sgsn-address, page 808
- bearer traffic-group, page 810
- cca quota-state, page 812
- cca redirect-indicator, page 814
- copy-packet-to-log, page 816
- description, page 817
- dns answer-name, page 818
- dns any-match, page 820
- dns previous-state, page 822
- dns query-name, page 824
- dns return-code, page 826
- dns state, page 828
- dns tid, page 830
- email, page 832
- end, page 835
- exit, page 836
- file-transfer any-match, page 837
- file-transfer chunk-number, page 839
- file-transfer current-chunk-length, page 841
- file-transfer declared-chunk-length, page 843
- file-transfer declared-file-size, page 845
- file-transfer filename, page 847
- file-transfer previous-state, page 849
- file-transfer state, page 851
- file-transfer transferred-file-size, page 853
- ftp any-match, page 855
- ftp client-ip-address, page 857
- ftp client-port, page 859
- ftp command args, page 861
- ftp command id, page 863
- ftp command name, page 865
- ftp connection-type, page 867
- ftp data-any-match, page 869
- ftp filename, page 871
- ftp pdu-length, page 873
• ftp pdu-type, page 875
• ftp previous-state, page 877
• ftp reply code, page 879
• ftp server-ip-address, page 881
• ftp server-port, page 883
• ftp session-length, page 885
• ftp state, page 887
• ftp url, page 889
• ftp user, page 891
• http accept, page 893
• http any-match, page 895
• http attribute-in-data, page 897
• http attribute-in-url, page 899
• http content disposition, page 901
• http content length, page 903
• http content range, page 905
• http content type, page 906
• http cookie, page 908
• http domain, page 910
• http error, page 912
• http first-request-packet, page 914
• http header-length, page 916
• http host, page 918
• http payload-length, page 921
• http pdu-length, page 923
• http previous-state, page 925
• http referer, page 927
• http reply code, page 930
• http reply payload, page 932
• http request method, page 933
• http session-length, page 935
• http state, page 937
• http transaction-length, page 939
- http transfer-encoding, page 941
- http uri, page 943
- http url, page 946
- http user-agent, page 949
- http version, page 951
- http x-header, page 953
- icmp any-match, page 955
- icmp code, page 957
- icmp type, page 959
- icmpv6 any-match, page 961
- icmpv6 code, page 963
- icmpv6 type, page 965
- if-protocol, page 967
- imap any-match, page 969
- imap cc, page 971
- imap command, page 973
- imap content class, page 975
- imap content type, page 977
- imap date, page 979
- imap final-reply, page 981
- imap from, page 983
- imap mail-size, page 985
- imap mailbox-size, page 987
- imap message-type, page 989
- imap previous-state, page 991
- imap session-length, page 993
- imap session-previous-state, page 995
- imap session-state, page 997
- imap state, page 999
- imap subject, page 1001
- imap to, page 1003
- ip any-match, page 1005
- ip dscp, page 1007
• ip downlink, page 1009
• ip dst-address, page 1011
• ip error, page 1013
• ip protocol, page 1015
• ip server-domain-name, page 1017
• ip server-ip-address, page 1019
• ip src-address, page 1021
• ip subscriber-ip-address, page 1023
• ip total-length, page 1025
• ip uplink, page 1027
• ip version, page 1029
• mms any-match, page 1030
• mms bcc, page 1032
• mms cc, page 1034
• mms content location, page 1036
• mms content type, page 1038
• mms downlink, page 1040
• mms from, page 1042
• mms message-id, page 1044
• mms pdu-type, page 1046
• mms previous-state, page 1048
• mms response status, page 1050
• mms state, page 1051
• mms status, page 1053
• mms subject, page 1054
• mms tid, page 1056
• mms to, page 1058
• mms uplink, page 1060
• mms version, page 1062
• multi-line-or all-lines, page 1064
• p2p any-match, page 1065
• p2p app-identifier, page 1067
• p2p behavioral, page 1069
• rtp pdu-length, page 1143
• rtp rtsp-id, page 1145
• rtp session-length, page 1147
• rtp uri, page 1149
• rtsp any-match, page 1151
• rtsp content length, page 1153
• rtsp content type, page 1155
• rtsp date, page 1157
• rtsp previous-state, page 1159
• rtsp reply code, page 1161
• rtsp request method, page 1163
• rtsp request packet, page 1165
• rtsp rtsp-seq, page 1167
• rtsp rtsp-time, page 1169
• rtsp rtsp-uri, page 1171
• rtsp session-id, page 1173
• rtsp session-length, page 1175
• rtsp state, page 1177
• rtsp uri, page 1179
• rtsp uri sub-part, page 1182
• rtsp user-agent, page 1185
• rtsp-stream any-match, page 1187
• rtsp-stream first-setup-url, page 1189
• rule-application, page 1192
• sdp any-match, page 1194
• sdp connection-ip-address, page 1196
• sdp media-audio-port, page 1198
• sdp media-video-port, page 1200
• sdp uplink, page 1202
• secure-http any-match, page 1204
• secure-http uplink, page 1206
• sip any-match, page 1208
• sip call-id, page 1210
ACS Ruledef Configuration Mode Commands

- sip content length, page 1212
- sip content type, page 1214
- sip from, page 1216
- sip previous-state, page 1218
- sip reply code, page 1220
- sip request method, page 1222
- sip request packet, page 1224
- sip state, page 1226
- sip to, page 1228
- sip uri, page 1230
- smtp any-match, page 1232
- smtp command arguments, page 1234
- smtp command id, page 1236
- smtp command name, page 1238
- smtp mail-size, page 1240
- smtp pdu-length, page 1242
- smtp previous-state, page 1244
- smtp recipient, page 1246
- smtp reply arguments, page 1248
- smtp reply id, page 1250
- smtp reply status, page 1252
- smtp sender, page 1254
- smtp session-length, page 1256
- smtp state, page 1258
- tcp analyzed out-of-order, page 1260
- tcp any-match, page 1262
- tcp client-port, page 1264
- tcp connection-initiator, page 1266
- tcp downlink, page 1267
- tcp dst-port, page 1269
- tcp duplicate, page 1271
- tcp either-port, page 1273
- tcp error, page 1275
• tcp flag, page 1277
• tcp initial-handshake-lost, page 1279
• tcp payload, page 1281
• tcp payload-length, page 1282
• tcp previous-state, page 1284
• tcp proxy-prev-state, page 1286
• tcp proxy-state, page 1288
• tcp server-port, page 1290
• tcp session-length, page 1292
• tcp src-port, page 1294
• tcp state, page 1296
• tcp uplink, page 1298
• tethering-detection, page 1300
• tftp any-match, page 1302
• tftp data-any-match, page 1304
• tls, page 1306
• udp any-match, page 1308
• udp client-port, page 1310
• udp downlink, page 1312
• udp dst-port, page 1314
• udp either-port, page 1316
• udp payload starts-with, page 1318
• udp server-port, page 1319
• udp src-port, page 1321
• udp uplink, page 1323
• wsp any-match, page 1325
• wsp content type, page 1327
• wsp domain, page 1329
• wsp downlink, page 1331
• wsp first-request-packet, page 1333
• wsp host, page 1335
• wsp pdu-length, page 1337
• wsp pdu-type, page 1339
• wsp previous-state, page 1341
• wsp reply code, page 1343
• wsp session-length, page 1345
• wsp session-management, page 1347
• wsp state, page 1349
• wsp status, page 1351
• wsp tid, page 1352
• wsp total-length, page 1353
• wsp transfer-encoding, page 1354
• wsp uplink, page 1356
• wsp url, page 1358
• wsp user-agent, page 1361
• wsp x-header, page 1363
• wtp any-match, page 1365
• wtp downlink, page 1367
• wtp gtr, page 1369
• wtp pdu-length, page 1371
• wtp pdu-type, page 1372
• wtp previous-state, page 1374
• wtp rid, page 1376
• wtp state, page 1378
• wtp tid, page 1380
• wtp transaction class, page 1381
• wtp ttr, page 1382
• wtp uplink, page 1384
• www any-match, page 1386
• www content type, page 1388
• www domain, page 1390
• www downlink, page 1392
• www first-request-packet, page 1394
• www header-length, page 1396
• www host, page 1398
• www payload-length, page 1400
• www pdu-length, page 1402
• www previous-state, page 1404
• www reply code, page 1406
• www state, page 1408
• www transfer-encoding, page 1410
• www url, page 1412
bearer 3gpp apn

This command allows you to define rule expressions to match Access Point Name (APN) of the bearer flow.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration  
```  
active-charging service service_name > ruledef ruledef_name  
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#  
```

**Syntax Description**

```  
| no | bearer 3gpp apn | case-sensitive | operator apn_name  
```

- **no**  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**  
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**  
  Specifies how to match.

  **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
**apn_name**

Specifies name of the APN to match.

*apn_name* must be an alphanumeric string of 1 through 62 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match an APN in the bearer flow.

**Examples**

The following command defines a rule expression to match user traffic based on APN named *apn12*:

```
bearer 3gpp = apn12
```
**bearer 3gpp imsi**

This command allows you to define rule expressions to match International Mobile Station Identification (IMSI) number in the bearer flow.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-chargingservice service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

```plaintext
| no | bearer 3gpp imsi { operator imsi | { !range | range } imsi-pool imsi_pool_name }
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- `!`: Does not equal
- `=`: Equals

**imsi**

Specifies the IMSI number to match.

**!range | range**

- `!range`: Not in the range of
- `range`: In the range of
**Usage Guidelines**

Use this command to define rule expressions to match an IMSI.

**Examples**

The following command defines a rule expression to analyze user traffic for the IMSI number 9198838330912:

```
bearer 3gpp imsi = 9198838330912
```
bearer 3gpp rat-type

This command allows you to define rule expressions to match Radio Access Technology (RAT) in the bearer flow.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | bearer 3gpp rat-type operator rat_type |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- ==: Equals

rat_type
Specifies the RAT type to match.
rat_type must be one of the following:

- geran: GSM EDGE Radio Access Network type
- utran: UMTS Terrestrial Radio Access Network type
- wlan: Wireless LAN type
Usage Guidelines

Use this command to define rule expressions to match a RAT type.

Examples

The following command defines a rule expression to match user traffic based on RAT type wlan:

```
bearer 3gpp rat-type = wlan
```
bearer 3gpp sgsn-address

This command allows you to define rule expressions to match SGSN address associated in the bearer flow.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description | no | bearer 3gpp sgsn-address operator ipv4/ipv6_address

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• ==: Equals

ipv4/ipv6_address

Specifies the SGSN IP address to match.

ipv4/ipv6_address must be in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines Use this command to define rule expressions to match IP address of an SGSN node. This command replaces the bearer sgsn-address command.
Examples

The following command defines a rule expression to analyze user traffic for an SGSN node with IP address 10.1.1.1:

```
bearer 3gpp sgsn-address = 10.1.1.1
```
### bearer 3gpp2 bsid

This command allows you to define rule expressions to match Base Station Identifier (BSID) associated with the bearer.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

| no | bearer 3gpp2 bsid | case-sensitive | use-group-of-objects | operator string |

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  - Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **use-group-of-objects**
  - Specifies using a group-of-objects as a qualifier to match this rule.

- **operator**
  - Specifies how to match.
  - **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
string

Specifies the name of a group-of-objects to match.

If the use-group-of-objects keyword is not included in the command, string specifies name of the matching 3GPP2 service Base Station ID (BSID) in bearer flow.

If the use-group-of-objects keyword is included in the command, string must be the name of the group-of-objects to use. In this case, it is checked if the rule is satisfied for either one or none of the objects in the group-of-objects depending upon the operator used. For example, if the operator is contains, the expression would be true if any of the objects in the specified object group is contained in the BSID. If the operator is !contains, then the expression would be true if none of the objects in the object group is contained in the BSID.

string must be an alphanumeric string of 1 through 16 characters, and may contain punctuation characters.

Usage Guidelines
Use this command to define rule expressions to match a 3GPP2 Base Station Identifier (BSID).

Examples
The following command defines a rule expression to analyze user traffic for 3GPP2 BSID named bs001_xyz:

```bash
bearer 3gpp2 bsid = bs001_xyz
```
bearer 3gpp2 service-option

This command allows you to define rule expressions to match 3GPP2 service with service options associated with the bearer.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs-ruledef) #

Syntax Description

| no | bearer 3gpp2 service-option operator service_option_code

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• >=: Greater than or equals

service_option_code

Specifies the 3GPP2 service option code to match.

service_option_code must be an integer from 0 through 1000.

Usage Guidelines

Use this command to define rule expressions to match a 3GPP2 service's service option code.
The following command defines a rule expression to analyze user traffic for a 3GPP2 service's service option matching 1034:
```plaintext
bearer 3gpp2 service-option = 1034
```
bearer apn

This command allows you to define rule expressions to match the APN used for the subscriber session.

Important

In 8.1 and later releases, this command is deprecated and is replaced by the bearer 3gpp apn command.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

[ no | bearer apn | case-sensitive ] operator apn_name

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.

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

**apn_name**

Specifies the APN to match.

*apn_name* must be the name of an APN, and must be an alphanumeric string of 1 through 62 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match APN used for subscriber session.

**Examples**

The following command defines a rule expression to match user traffic based on APN name *apn12*:

```
bearer apn = apn12
```
**bearer imsi**

This command allows you to define rule expressions to match IMSI number of the subscriber.

In 8.1 and later releases, this command is deprecated and is replaced by the `bearer 3gpp imsi` command.

### Product

ACS

### Privilege

Security Administrator, Administrator

### Command Modes

`Exec > ACS Configuration > Ruledef Configuration`

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

### Syntax Description

```
[ no ] bearer imsi { operator imsi | { !range | range } imsi-pool imsi_pool_name }
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `=`: Equals

- **imsi**
  Specifies the IMSI number to match.

- **!range | range**
  Specifies the range criteria:
  
  - `!range`: Not in the range of
• **range**: In the range of

```plaintext
imsi-pool imsi_pool_name
```

Specifies an IMSI pool.

`imsi_pool_name` must be the name of an IMSI pool, and must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to define rule expressions to match IMSI number of subscriber.

**Examples**

The following command defines a rule expression to match user traffic based on IMSI number 919883830912:

```plaintext
bearer imsi = 919883830912
```
**bearer rat-type**

This command allows you to define rule expressions to match Radio Access Technology (RAT) in the bearer flow.

---

**Important**

In 8.1 and later releases, this command is deprecated and is replaced by the command.

---

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```plaintext
| no | bearer rat-type operator rat_type
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `==`: Equals

- **rat_type**
  - Specifies the RAT type to match.
  - `rat_type` must be one of the following:
    - `geran`: GSM EDGE Radio Access Network type
    - `utran`: UMTS Terrestrial Radio Access Network type
• wlan: Wireless LAN type

Usage Guidelines
Use this command to define rule expressions to match a RAT type.

Examples
The following command defines a rule expression to match user traffic based on RAT type wlan:

```
bearer rat-type = wlan
```
bearer sgsn-address

This command allows you to define rule expressions to match IP address of the SGSN (in acting as GGSN) / P-GW (if acting as S-GW) in the bearer flow.

Important

In 8.1 and later releases, this command is deprecated and is replaced by the command.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef)#

Syntax Description

| no | bearer sgsn-address operator ipv4/ipv6_address

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- ==: Equals

ipv4/ipv6_address

Specifies the SGSN IP address to match.

ipv4/ipv6_address must be in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Use this command to define rule expressions to match IP address of the SGSN (in acting as GGSN) / P-GW (if acting as S-GW).
Examples

The following command defines a rule expression to match user traffic based on SGSN node IP address 10.1.1.1:

```
bearer sgsn-address = 10.1.1.1
```
bearer traffic-group

This command allows you to define rule expressions to match traffic group number associated with the subscriber session.

Important

This functionality is available only if the Content Access Control license has been installed on the chassis.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef) #

Syntax Description

| no | bearer traffic-group operator group_number

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• <=: Lesser than or equals
• =: Equals
• >=: Greater than or equals

group_number

Specifies the traffic group number to match.

group_number must be an integer from 1 through 255.
Usage Guidelines

Use this command to define rule expressions to match traffic group of the subscriber session. See the `fa-ha-spi` command in the *HA Service Configuration Mode Commands* chapter for more information.

Examples

The following command defines a rule expression to analyze all traffic groups assigned a value greater or equal to 23:

```
bearer traffic-group >= 23
```
cca quota-state

Specifies the quota state of a subscriber for prepaid credit control service. In release 12.0 and later, this command should be used as a post-processing rule. For more information on post-processing policy command, refer to the ACS Rulebase Configuration Mode Commands chapter in this guide.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] cca quota-state operator { limit-reached | lower-bandwidth }
```

**no**
Disables the configured credit control quota state.

**operator**

Specifies how to match.

`operator` must be one of the following:

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `=`: Equals
- `>=`: Greater than or equals

**limit-reached**

This state matches an affirmative end-of-quota indication for the current ruledef from the prepay server.

**lower-bandwidth**

This state matches the lower-bandwidth quota state of a rating group.
Usage Guidelines

This command supports URL redirection 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 be applied via the `cca quota-state` command.

Examples

The following command defines a rule expression to match user traffic based on the Credit-Control Application (CCA) quota state `limit-reached`:

```
cca quota-state = limit-reached
```
**cca redirect-indicator**

This command allows you to define rule expressions to match redirect-indicator state of the Credit Control Application. In release 12.0 and later, this command should be used as a post-processing rule. For more information on post-processing policy command, refer to *ACS Rulebase Configuration Mode Commands* chapter in this reference.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

*active-charging service service_name > ruledef ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | cca redirect-indicator operator redirect_indicator
```

**no**

Disables the configured CCA redirect-indicator in the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- !: Does not equal
- <=: Lesser than or equals
- =: Equals
- >=: Greater than or equals

**redirect_indicator**

Specifies the redirect indicator for the AVP used for redirection of the URL in the RADIUS dictionary for prepaid service. It must be an integer from 0 through 4294967295.
For the RADIUS server configured with different values to return for this AVP, the ACS requires ruledefs to match the different values for system to associate with charging actions that have different redirect URLs configured.

**Usage Guidelines**

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 the 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.

**Examples**

The following command defines a rule expression to match redirect indicator 1234 for the URL Redirect AVP:

```
cca redirect-indicator = 1234
```
copy-packet-to-log

This command allows you to print every packet that hits the current ruledef to a log statement.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**

| no | copy-packet-to-log

**no**

Disables the copy-packet-to-log feature.

**copy-packet-to-log**

Specifies to print packets hitting the current ruledef to a log.

**Usage Guidelines**

Use this command to print every packet that hits a ruledef to a log statement. This facilitates debugging.
description

Allows you to enter descriptive text for this configuration.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

description text

no description

no
Clears the description for this configuration.

text
Enter descriptive text as an alphanumeric string of 1 to 100 characters.
If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

Usage Guidelines

The description should provide useful information about this configuration.
dns answer-name

This command allows you to define rule expressions to match answer name in the answer section of DNS response messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
nodns answer-name [case-sensitive] operator value
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  **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 value to match.

value must be an alphanumeric string of 1 through 255 characters and may contain punctuation characters.

Usage Guidelines

Use this command to define rule expressions to match an answer name from the answer section of DNS response messages.

The answer section of a DNS response may contain more than one answer. A maximum of seven answers from the response packet are parsed. For the equality expressions (=, contains, starts-with, ends-with) a match is sought from any of the answers in the packet (up to the first seven answers). For the inequality expressions (!=, !contains, !starts-with, !ends-with), a non-match is sought from all answers (up to the first seven answers).

Examples

The following command defines a rule expression to match user traffic for answer name test:

dns answer-name = test
**dns any-match**

This command allows you to define rule expressions to match all DNS packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | dns any-match operator condition
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.
  
  - `!=`: Does not equal
  - `==`: Equals

- **condition**
  
  Specifies the condition to match.
  
  - `FALSE`
  - `TRUE`

**Usage Guidelines**

Use this command to define an any-match rule expression to match all DNS packets.
Examples

The following command defines an any-match rule expression to match all DNS packets:

dns any-match = TRUE
**dns previous-state**

This command allows you to define rule expressions to match previous state of the DNS FSM.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

*active-charging service service_name > ruledef ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | dns previous-state operator dns previous_state
```

no

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- !:= Does not equal
- := Equals

**dns previous_state**

Specifies the previous state to match.

*dns previous_state* must be one of the following:

- dns-timeout
- init
- req-sent
- resp-error
- resp-success
Usage Guidelines

Use this command to define rule expressions to match previous state of DNS FSM.

Examples

The following command defines a rule expression to match the DNS FSM previous state \texttt{req-sent}:
\begin{verbatim}
dns previous-state = req-sent
\end{verbatim}
**dns query-name**

This command allows you to define rule expressions to match query name in DNS request messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | dns query-name | case-sensitive | operator query_name |

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**case-sensitive**
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

**operator**
Specifies how to match.

`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
**query_name**

Specifies the query name to match.

*query_name* must be an alphanumeric string of 1 through 255 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match query name in DNS request messages.

**Examples**

The following command defines a rule expression to match DNS query name *test*:

```
dns query-name = test
```
dns return-code

This command allows you to define rule expressions to match response code in DNS response messages.

Product ACS

Privilege Security Administrator, Administrator

Command Modes

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | dns return-code operator return_code

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• ==: Equals

return_code
Specifies the response code to match.
return_code must be one of the following:

• format-error
• name-error
• no-error
• not-implemented
• refused
Usage Guidelines
Use this command to define rule expressions to match response code in DNS response messages.

Examples
The following command defines a rule expression to match a DNS response code refused:

dns return-code = refused
dns state

This command allows you to define rule expressions to match current state of DNS FSM.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs-ruledef) #

Syntax Description

| no | dns state operator dns_current_state |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• =: Equals

dns_current_state
Specifies the current state to match.
dns_current_state must be one of the following:

• dns-timeout
• init
• req-sent
• resp-error
• resp-success
Usage Guidelines

Use this command to define rule expressions to match DNS FSM current state.

Examples

The following command defines a rule expression to match DNS FSM current state of `req-sent`:

dns state = req-sent
dns tid

This command allows you to define rule expressions to match Transaction Identifier (TID) field in DNS messages.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef) #

Syntax Description

| no | dns tid operator tid_value

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

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 to match.

tid_value must be an integer from 1 through 65535.

Usage Guidelines

Use this command to define rule expressions to match a TID field of DNS messages.
Examples

The following command defines a rule expression to match DNS TID field value of test:

dns tid = test
This command allows you to define rule expressions to match generic e-mail message parameters. These expressions will be applicable for IMAP, MMS, POP3, and SMTP protocols.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | email { cc | content { class | type } | from | size | subject | to } | case-sensitive | operator value
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **cc**
  
  Specifies to match the "cc" field of standard e-mail message.

- **content { class | type }**
  
  Specifies to match the "content-type" or "content-class" field of standard e-mail message.

- **from**
  
  Specifies to match the "from" field of standard e-mail message.

- **subject**
  
  Specifies to match the "subject" field of standard e-mail message.

- **to**
  
  Specifies to match the "to" field of standard e-mail message.
**size**
Specifies to match with the total size of e-mail message specified in bytes.

**case-sensitive**
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

**operator**
Specifies how to match.

*operator* must be one of the following except for *size*:

- !=: 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

*operator* must be one of the following for *size*:

- !=: Does not equal
- <=: Lesser than or equals
- =: Equals
- >=: Greater than or equals

**value**
Specifies the value to match.

*value* must be an alphanumeric string and can contain punctuation characters.

- cc: A string of 1 through 512 characters
- content: A string of 1 through 128 characters
- from: A string of 1 through 64 characters
- size: A range of bytes from 1 through 4000000000 bytes
- subject: A string of 1 through 128 characters
- to: A string of 1 through 512 characters

**Usage Guidelines**
Use this command to define rule expressions to match different fields/parameters within standard e-mail messages.
The following command defines a rule expression to analyze user traffic for the occurrence of triangle in the "cc" field of e-mail messages:

```plaintext
e-mail cc contains triangle@xyz.com
```
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax Description
end

Usage Guidelines
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 Description**

`exit`

**Usage Guidelines**

Use this command to return to the parent configuration mode.
file-transfer any-match

This command allows you to define rule expressions to match all file-transfer packets. This expression applies to file transfers that use the FTP or HTTP protocols.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```plaintext
| no | file-transfer any-match operator condition |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  Specifies the condition to match.
  - `FALSE`
  - `TRUE`

**Usage Guidelines**

Use this command to define rule expressions to match all file-transfer packets. This expression applies to file transfers that use the FTP or HTTP protocols.
Examples

The following command defines a rule expression to match all file-transfer packets:

```
file-transfer any-match = TRUE
```
file-transfer chunk-number

This command allows you to define rule expressions to match the total number of chunks in an HTTP file as determined by the File Transfer analyzer.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```plaintext
| no | file-transfer chunk-number operator chunks_number
```

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `==`: Equals
- `>=`: Greater than or equals

**chunks_number**
Specifies the number of chunks to match.

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

**Usage Guidelines**
Use this command to define rule expressions to match the total number of chunks in an HTTP file as determined by the File Transfer analyzer.
Examples

The following command defines a rule expression to match 150 number of chunks:

```
file-transfer chunk-number = 150
```
file-transfer current-chunk-length

This command allows you to define rule expressions to match the length of an HTTP chunk currently in the File Transfer analyzer.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**active-charging service service_name > ruledef ruledef_name**

Entering the above command sequence results in the following prompt:

[local]\host_name{config-acs-ruledef}#

**Syntax Description**

| no | file-transfer current-chunk-length operator current_chunk_length |

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

**current_chunk_length**

Specifies the current chunk length value (in bytes) to match.

*current_chunk_length* must be an integer from 1 through 40000000.

**Usage Guidelines**

Use this command to define rule expressions to match the length of an HTTP chunk currently in the File Transfer analyzer.
Examples

The following command defines a rule expression to match length of current HTTP chunk as 1500000 bytes:

```
file-transfer current-chunk-length = 1500000
```
**file-transfer declared-chunk-length**

This command allows you to define rule expressions to match the declared length of an HTTP chunk currently in the File Transfer analyzer.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax Description**

```
| no | file-transfer declared-chunk-length operator declared_chunk_length
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**operator** must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- =: Equals
- >=: Greater than or equals

**declared_chunk_length**

Specifies the declared chunk length value (in bytes) to match.

**declared_chunk_length** must be an integer from 1 through 40000000.

**Usage Guidelines**

Use this command to define rule expressions to match the declared length of an HTTP chunk currently in the File Transfer analyzer.
Examples

The following command defines a rule expression to match declared length of the current HTTP chunk as 2500000 bytes:

file-transfer declared-chunk-length = 2500000
file-transfer declared-file-size

This command allows you to define rule expressions to match the declared file size by the File Transfer analyzer decoding the FTP handshake.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[no] file-transfer declared-file-size operator declared_file_size
```

*no*

If previously configured, deletes the specified rule expression from the current ruledef.

*operator*

Specifies how to match.

*operator* must be one of the following:

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `==`: Equals
- `>=`: Greater than or equals

*declared_file_size*

Specifies the declared file size (in bytes) to match.

*declared_file_size* must be an integer from 1 through 40000000.

**Usage Guidelines**

Use this command to define rule expressions to match the declared file size by the File Transfer analyzer decoding the FTP handshake.
Examples

The following command defines a rule expression to match declared file size as 2500000 bytes:

```
file-transfer declared-file-size = 2500000
```
**file-transfer filename**

This command allows you to define rule expressions to match file name.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
no | file-transfer filename | case-sensitive | operator file_name
```

- **no**  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**  
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**  
  Specifies how to match.

  - **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
**file-transfer filename**

Specifies the file name to match.

`file_name` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match file name in file-transfer.

**Examples**

The following command defines a rule expression to match file name containing `star1`:

```
file-transfer filename contains star1
```
file-transfer previous-state

This command allows you to define rule expressions to match previous state of File Transfer FSM.

**Product** ACS

**Privilege** Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

[ no ] file-transfer previous-state operator file_transfer_previous_state

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- !=: Does not equal
- =: Equals

**file_transfer_previous_state**

Specifies the previous state to match.

*file_transfer_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 Guidelines
Use this command to define rule expressions to match previous state of File Transfer FSM.

Examples
The following command defines a rule expression to match previous state of *init*:

```
file-transfer previous-state = init
```
file-transfer state

This command allows you to define rule expressions to match the current state of File Transfer FSM.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description

| no | file-transfer state operator file_transfer_current_state

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

 Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• ==: Equals

file_transfer_current_state

Specifies the current state to match.

file_transfer_current_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 Guidelines

Use this command to define rule expressions to match current state of File Transfer FSM.

The following table describes 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>

Examples

The following command defines a rule expression to match file-transfer current state of init:

```
file-transfer state = init
```
file-transfer transferred-file-size

This command allows you to define rule expressions to match the size of a file that has been transferred so far, as detected by the File Transfer analyzer.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

**active-charging service service_name > ruledef ruledef_name**

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef) #

**Syntax Description**

| no | file-transfer transferred-file-size operator transferred_file_size |

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**operator** must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

**transferred_file_size**

Specifies the transferred file size (in bytes) to match.

**transferred_file_size** must be an integer from 1 through 4000000000.

**Usage Guidelines**

Use this command to define rule expressions to match the size of the file that has been transferred so far, as detected by the File Transfer analyzer.
Examples

The following command defines a rule expression to match file transferred size of 2500 bytes:

```
file-transfer transferred-file-size = 2500
```
**ftp any-match**

This command allows you to define rule expressions to match all FTP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | ftp any-match operator condition |
```

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

- `!=`: Does not equal
- `==`: Equals

**condition**
Specifies the condition to match.

- `FALSE`
- `TRUE`

**Usage Guidelines**
Use this command to define a rule expression to match all FTP packets.
The following command defines a rule expression to match all FTP packets:

```
ftp any-match = TRUE
```
**ftp client-ip-address**

This command allows you to define rule expressions to match IP address of the FTP client.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax Description**

```
[ no ] ftp client-ip-address operator ipv4/ipv6_address
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.

- **operator** must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- **ipv4/ipv6_address**
  Specifies the FTP client IP address to match.

  `ipv4/ipv6_address` must be in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage Guidelines**

Use this command to define rule expressions to match an FTP client IP address, which will be either the IP source address or the IP destination address, depending on the direction.
Examples

The following command defines a rule expression to match client IP address 10.1.1.1:

```
ftp client-ip-address = 10.1.1.1
```
**ftp client-port**

This command allows you to define rule expressions to match port number of the FTP client.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

*active-charging service service_name > ruledef ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax Description**

| no | ftp client-port operator port_number |

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  - **operator** must be one of the following:
    - `!=`: Does not equal
    - `<=`: Lesser than or equals
    - `=`: Equals
    - `>=`: Greater than or equals

- **port_number**
  
  Specifies the client port number to match.

  - **port_number** must be an integer from 1 through 65535.

**Usage Guidelines**

Use this command to define rule expressions to match port number of the FTP client, which will be either the TCP source port or the TCP destination port, depending on the direction.
Examples

The following command defines a rule expression to match FTP client port number 10:

\texttt{ftp client-port = 10}
**ftp command args**

This command allows you to define rule expressions to match arguments within an FTP command.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```text
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```text
[ no ] ftp command args | case-sensitive | operator argument
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  **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 argument to match. 

*argument* must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to define rule expressions to match arguments within an FTP command.

**Examples**

The following command defines a rule expression to match argument *ascii* within an FTP command:

`ftp command args = ascii`
ftp command id

This command allows you to define rule expressions to match FTP command ID.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax Description**

```
| no | ftp command id operator command_id
```

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

operator must be one of the following:

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `>=`: Greater than or equals
- `==`: Equals

**command_id**
Specifies the command identifier to match.

In 8.3 and earlier releases, command_id must be an integer from 0 through 15.
In 9.0 and later releases, command_id must be an integer from 0 through 18.

**Usage Guidelines**
Use this command to define rule expressions to match FTP command ID.
Examples

The following command defines a rule expression to match the FTP command ID 10:

\texttt{ftp command id = 10}
ftp command name

This command allows you to define rule expressions to match FTP command name.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs-ruledef) #

Syntax Description

| no | ftp command name operator command_name |

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**operator** must be one of the following:

- !=: Does not equal
- ==: Equals

**command_name**

Specifies the command name to match.

**command_name** must be one of the following:

- abor: Abort command
- cwd: Current working directory command
- epri: epri command
- epsv: epsv command
- list: List command
- **mode**: Transfer mode command
- **pass**: Password command
- **pasv**: Passive command
- **port**: Port command
- **quit**: Quit command
- **rest**: Restore command
- **retr**: Retry command
- **stor**: Store command
- **stru**: File structure command
- **syst**: System command
- **type**: Type command
- **user**: User command

**Usage Guidelines**
Use this command to define rule expressions to match FTP command name.

**Examples**
The following command defines a rule expression to match FTP command name `list`:

```
ftp command name = list
```
**ftp connection-type**

This command allows you to define rule expressions to match FTP connection type.

**Command Modes**

```
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] ftp connection-type operator connection_type
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**

  Specifies how to match.

  `operator` must be one of the following:

  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **connection_type**

  Specifies the connection type to match.

  `connection_type` must be one of the following:

  - `0`: Unknown
  - `1`: Control connection
  - `2`: Data connection

---

**Product**

ACS

**Privilege**

Security Administrator, Administrator
Usage Guidelines

Use this command to define rule expressions to match an FTP connection type.

Examples

The following command defines a rule expression to match FTP connection type 1:

`ftp connection-type = 1`
ftp data-any-match

This command allows you to define rule expressions to match all FTP data packets.

**Product** ACS

**Privilege** Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | ftp data-any-match operator condition |

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**condition**

Specifies the condition to match.

**Usage Guidelines**

Use this command to define rule expressions to match all FTP data packets.
Examples

The following command defines a rule expression to match all FTP data packets:

```
ftp data-any-match = TRUE
```
ftp filename

This command allows you to define rule expressions to match FTP file name.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local] host_name(config-acs-ruledef)#

Syntax Description
| no | ftp filename | case-sensitive | operator file_name |

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
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
**file_name**

Specifies the file name to match.

*file_name* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match an FTP file name.

**Examples**

The following command defines a rule expression to match a file named *testtransfer*:

```
ftp filename = testtransfer
```
**ftp pdu-length**

This command allows you to define rule expressions to match the length of a current FTP packet.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | ftp pdu-length operator pdu_length |

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

**pdu_length**

Specifies the FTP PDU length (in bytes) to match.

*pdu_length* must be an integer from 0 through 65535.

**Usage Guidelines**

Use this command to define rule expressions to match the length of a current FTP packet, that is, FTP PDU length (FTP header + FTP payload).
Examples

The following command defines a rule expression to match an FTP PDU length of 9647 bytes:

\texttt{ftp pdu-length = 9647}
**ftp pdu-type**

This command allows you to define rule expressions to match FTP Protocol Data Unit (PDU) type.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

    active-charging service *service_name* > ruledef *ruledef_name*

Entering the above command sequence results in the following prompt:

    [local] *host_name* (config-acs-ruledef) #

**Syntax Description**

    | no | ftp pdu-type *operator* *pdu_type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

*operator*

Specifies how to match.

*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 to match.

*pdu_type* must be one of the following:

- 0: Unknown
- 1: Command
- 2: Reply
Usage Guidelines  Use this command to define rule expressions to match a PDU type of FTP packet.

Examples  The following command defines a rule expression to match FTP PDU type 1:
ftp pdu-type = 1
**ftp previous-state**

This command allows you to define rule expressions to match previous state of FTP session.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef)#
```

**Syntax Description**

```plaintext
[ no ] ftp previous-state operator ftp_previous_state
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.
  
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `=`: Equals

- **ftp_previous_state**
  
  Specifies the previous state to match.
  
  `ftp_previous_state` must be one of the following:
  
  - `command-sent`
  - `init`
  - `response-error`
  - `response-ok`
**Usage Guidelines**

Use this command to define rule expressions to match a previous state of FTP session.

**Examples**

The following command defines a rule expression to match previous FTP state `init`:

```
ftp previous-state = init
```
**ftp reply code**

This command allows you to define rule expressions to match FTP reply code.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] ftp reply code operator reply_code
```

*no*

If previously configured, deletes the specified rule expression from the current ruledef.

*operator*

Specifies how to match.

*operator* must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

*reply_code*

Specifies the FTP reply code to match.

*reply_code* must be an integer from 100 through 599.

**Usage Guidelines**
Use this command to define rule expressions to match an FTP reply code.
The following command defines a rule expression to match FTP reply code 150:

```
ftp reply code = 150
```
**ftp server-ip-address**

This command allows you to define rule expressions to match FTP server IP address.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | ftp server-ip-address operator ipv4/ipv6_address
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - **operator** must be one of the following:
    - `!=`: Does not equal
    - `<=`: Lesser than or equals
    - `==`: Equals
    - `>=`: Greater than or equals

- **ipv4/ipv6_address**
  - Specifies IP address of the server to match
  - **ipv4/ipv6_address** must be in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage Guidelines**

Use this command to define rule expressions to match an FTP server IP address, which will be either the IP source address or the IP destination address, depending on the direction.
Examples

The following command defines a rule expression to match the FTP server IP address 10.1.1.1:

```plaintext
ftp server-ip-address = 10.1.1.1
```
### ftp server-port

This command allows you to define rule expressions to match FTP server port number.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration

```  
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax Description**  
| no | ftp server-port operator port |

- **no**  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**  
  Specifies how to match.
  
  **operator** must be one of the following:
  
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **port**  
  Specifies the FTP server port number to match.
  
  **port** must be an integer from 1 through 65535.

**Usage Guidelines**  
Use this command to define rule expressions to match an FTP server port number, which will be either the TCP source port or the TCP destination port, depending on the direction.
Examples

The following command defines a rule expression to analyze user traffic for FTP server port 21:

```
ftp server-port = 21
```
**ftp session-length**

This command allows you to define rule expressions to match the total number of bytes sent on an FTP control connection.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | ftp session-length operator session_length
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **session_length**
  Specifies the FTP session length (in bytes) to match.
  `session_length` must be an integer from 1 through 400000000.

**Usage Guidelines**
Use this command to define rule expressions to match the total number of bytes sent on an FTP control connection.
Examples

The following command defines a rule expression to match FTP session length of 40000 bytes:

```
ftp session-length = 40000
```
**ftp state**

This command allows you to define rule expressions to match the current state of an FTP session.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | ftp state operator ftp_state |

no

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**operator** must be one of the following:

- !=: Does not equal
- =: Equals

**ftp_state**

Specifies the FTP state to match.

**ftp_state** must be one of the following:

- close: FTP transmissions that are in closed state.
- command-sent: FTP transmissions that are in command-sent state.
- response-error: FTP transmissions that are in response-error state.
- response-ok: FTP transmissions that are in response-ok state.
Usage Guidelines

Use this command to define rule expressions to match the current state of an FTP session.

Examples

The following command defines a rule expression to match FTP current state close:

ftp state = close
**ftp url**

This command allows you to define rule expressions to match the FTP URL/path of a file being transferred.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | ftp url | case-sensitive | operator url |
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  - Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  - Specifies how to match.
  - `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

Specifies the URL to match.

_url_ must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to define rule expressions to match the FTP URL/path of a file being transferred.

**Examples**

The following command defines a rule expression to match the URL `ftp://rfc.ietf.org/rfc/rfc1738.txt`:

```
ftp url = ftp://rfc.ietf.org/rfc/rfc1738.txt
```
ftp user

This command allows you to define rule expressions to match the user name FTP command packet.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description
[ no ] ftp user [ case-sensitive ] operator ftp_user

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
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
ftps_user

Specifies the FTP user name to match.

*ftps_user* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match a user name FTP command.

**Examples**

The following command defines a rule expression to match FTP user name *user1*:

```
ftps user = user1
```
http accept

This command allows you to define rule expressions to match content types that are acceptable for the response.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef)#

**Syntax Description**

| no | http accept | case-sensitive | operator accept_field |

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  **operator** must be one of the following:
  - !=: Does not equal
  - !contains: Does not contain
  - !ends-with: Does not end with
  - !present: Not present
  - !starts-with: Does not start with
  - =: Equals
  - contains: Contains
  - ends-with: Ends with
• **present**: Present

• **starts-with**: Starts with

**accept_field**

Specifies the ACCEPT field present in the HTTP header to be matched.

*accept_field* must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to define rule expressions to match content types in the HTTP header that are acceptable for the response.

**Examples**

The following command defines a rule expression to match content that contains *cisco* in HTTP ACCEPT field:

**http accept contains cisco**
http any-match

This command allows you to define rule expressions to match all HTTP and HTTPS Connect Method packets.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

`[local]host_name(config-acs-ruledef)#`

Syntax Description

```
| no | http any-match operator condition |
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**operator** must be one of the following:

- `!=`: Does not equal
- `=`: Equal

**condition**

Specifies the condition to match.

**condition** must be one of the following:

- `FALSE`
- `TRUE`

Usage Guidelines Use this command to define rule expressions to match all HTTP packets.
The following command defines a rule expression to match all HTTP packets:

```
http any-match = TRUE
```
http attribute-in-data

This command allows you to define rule expressions to match any arbitrary attribute in the payload following the HTTP headers.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```bash
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[no] http attribute-in-data attribute | case-sensitive | operator value
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **attribute**
  
  `attribute` must be an alphanumeric string of 1 through 31 characters.

- **case-sensitive**
  
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  
  Specifies how to match.

  `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
**http attribute-in-data**

- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

**value**

Specifies the value as an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to define rule expressions to match arbitrary attribute in the payload following the HTTP headers.

In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.
http attribute-in-url

This command allows you to define rule expressions to match arbitrary attribute in the combined Host+URI HTTP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | http attribute-in-url attribute | case-sensitive | operator value |
```

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**attribute**
`attribute` must be an alphanumeric string of 1 through 31 characters.

**case-sensitive**
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

**operator**
Specifies how to match.

`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 value as an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to configure rule expression to match an arbitrary attribute in the combined Host+URI HTTP headers.

In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.
http content disposition

This command allows you to define rule expressions to match optional content-disposition field of HTTP entity header.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | http content disposition | case-sensitive | operator content_disposition |
```

| no |
If previously configured, deletes the specified rule expression from the current ruledef.

| case-sensitive |
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

| operator |
Specifies how to match.

`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_disposition**

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_disposition* must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match optional content-disposition field of HTTP entity header. This feature supports RFC 2616 for HTTP and RFC 1806 for Content Disposition.

In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

**Examples**

The following command defines a rule expression to match content disposition *successful*:

```plaintext
http content disposition = successful
```
http content length

This command allows you to define rule expressions to match the value in HTTP Content-Length entity-header field.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | http content length operator content_length |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• >=: Greater than or equals

content_length
Specifies the HTTP body length (in bytes) to match.
content_length must be an integer from 1 through 4000000000.

Usage Guidelines
Use this command to define rule expressions to match value in HTTP Content-Length entity-header field.
In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

**Examples**

The following command defines a rule expression to match value of 10000 bytes in HTTP Content-Length entity-header field:

```
http content length = 10000
```
http content range

This command allows you to define rule expressions for CAE re-addressing to verify if the HTTP Response has content-range header or not.

**Important**

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product**

ACS
MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

`[no] http content range = TRUE`

*no*

If previously configured, deletes the specified rule expression from the current ruledef.

**Usage Guidelines**

Use this command to define rule expressions for CAE re-addressing to verify if the HTTP Response has content-range header or not. This header is useful in detecting HTTP video requests when using ECS DPI ruledefs based on HTTP headers/URI.
http content type

This command allows you to define rule expressions to match value in HTTP Content-Type entity-header field.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] <host_name>(config-acs-ruledef)#

**Syntax Description**

| no | http content type | case-sensitive | operator content_type |

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**case-sensitive**

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

**operator**

Specifies how to match.

* 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 content type to match.

*content_type* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match value in HTTP Content-Type entity-header field.

In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

**Examples**

The following command defines a rule expression to match *abc100* in HTTP Content-Type entity-header field:

```
http content type = abc100
```
http cookie

This command allows you to define rule expressions to match strings in the HTTP cookie header.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
| no | http cookie | case-sensitive | operator cookie_string |

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !present: Not present
• !starts-with: Does not start with
• =: Equals
• contains: Contains
• ends-with: Ends with
- **present**: Present
- **starts-with**: Starts with

**cookie_string**

Specifies the string to match in the HTTP cookie header. `cookie_string` must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to define rule expressions to match strings in an HTTP cookie header.

The cookie match rule line can be combined with other rule lines having different match criteria. Multiple line cookie header strings can be combined together using a comma (,) separator.

---

**Important**

The HTTP parser can parse up to a maximum of 4096 bytes in the cookie header. In the case of multiple line cookie headers, the maximum of 4096 bytes includes the total size of all cookie header values, and the separators added to combine them.

---

**Examples**

The following command defines a rule expression to match the HTTP cookie header with the string `tollfree`:

```
http cookie = tollfree
```
http domain

This command allows you to define rule expressions to match the domain portion of URIs in HTTP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef) #

Syntax Description
| no | http domain | case-sensitive | operator domain |

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
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
**domain**

Specifies the domain to match.

*domain* must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to define rule expressions to match the domain portion of URIs in HTTP packets. From the URL, after http:// (if present) is removed, everything until the first "/" is the domain.

**Examples**

The following command defines a rule expression to match user traffic based on domain name *testdomain*:

```
http domain = testdomain
```
http error

This command allows you to define rule expressions to match for errors in HTTP packets (for example, invalid HTTP header) and errors in the HTTP analyzer FSM (Finite State Machine) while parsing HTTP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description
| no | http error operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• =: Equals

condition
Specifies the condition to match.
condition must be one of the following:

• FALSE
• TRUE
Usage Guidelines

Use this command to define rule expressions to match for errors in HTTP packets and other errors in HTTP analyzer FSM while parsing HTTP packets. For example, FSM error, invalid header field values, ACS memory and buffer limit, packet related errors, and so on.

ACS 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.

In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

Examples

The following command defines a rule expression to match user traffic based on HTTP error status of TRUE:

```
http error = TRUE
```
**http first-request-packet**

This command allows you to define rule expressions to match the GET or POST request, if it is the first HTTP request for the subscriber's session.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | http first-request-packet operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  operator must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  Specifies the condition to match.
  condition must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage Guidelines**

Use this command to define rule expressions to match the GET or POST request, if it is the first HTTP request for the subscriber's session.
This expression can be connected with a charging action, so the subscriber is redirected to a splash page for the first Web access attempted.

**Examples**

The following command defines a rule expression to match first-request-packet:

```
http first-request-packet = TRUE
```
http header-length

This command allows you to define rule expressions to match HTTP header length.

Product ACS

Privilege Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | http header-length operator header_length

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- =: Equals
- >=: Greater than or equals

header_length
Specifies the HTTP header length (in bytes) to match.

header_length must be an integer from 0 through 65535.

Usage Guidelines

Use this command to define rule expressions to match the length of an HTTP header.

In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.
**Examples**

The following command defines a rule expression to match an HTTP header length of 8000:

`http header-length = 8000`
http host

This command allows you to define rule expressions to match value in HTTP Host request-header field.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | http host | case-sensitive | operator host_name |

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.

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
- regex: Regular expression
• **starts-with**: Starts with

**host_name**

Specifies the host name to match.

*host_name* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

### Usage Guidelines

Use this command to define rule expressions to match value in HTTP Host request-header field.

In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the *Enhanced Charging Service Administration Guide*.

### Table 6: Special Characters Supported in Regex Rule Expressions

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>(?)</td>
<td>Match zero or one character</td>
</tr>
<tr>
<td>?</td>
<td>Match the question mark (&lt;ctrl-v&gt;?).</td>
</tr>
<tr>
<td>+</td>
<td>Match the plus character</td>
</tr>
<tr>
<td>\*</td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td>\a</td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td>\b</td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td>\f</td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
</tbody>
</table>

**Command Line Interface Reference, Commands A - B, StarOS Release 20**
<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\n</td>
<td>Match the New line (ASCII 10) character</td>
</tr>
<tr>
<td>\r</td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td>\t</td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td>\v</td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td>\0</td>
<td>Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td>\</td>
<td>Match the backslash character</td>
</tr>
</tbody>
</table>

Bracketed range [0-9] Match any single character from the range

A leading ^ in a range Do not match any in the range. All other characters represent themselves.

\x## Any ASCII character as specified in two-digit hex notation.
For example, \x5A yields a "Z".

<table>
<thead>
<tr>
<th></th>
<th>Specify OR regular expression operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>Important When using the regex operator &quot;</td>
</tr>
</tbody>
</table>

Examples

The following command defines a rule expression to match host1 in HTTP Host request-header field:

```
http host = host1
```

The following command defines a regex rule expression to match either of the following values in the HTTP Host request-header field: host1, host23w01.

```
http host regex "host1|host23w01"
```
http payload-length

This command allows you to define rule expressions to match HTTP payload length.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration  
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax Description**  

```
[ no ] http payload-length operator payload_length
```

- **no**  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**  
  Specifies how to match.
  
  **operator** must be one of the following:

  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- **payload_length**  
  Specifies the HTTP payload (data) length (in bytes) to match.
  
  `payload_length` must be an integer from 1 through 4000000000.

**Usage Guidelines**  

Use this command to define rule expressions to match HTTP payload (data) length (pdu-length - header-length).
Examples

The following command defines a rule expression to match HTTP payload length of 100000 bytes:

```
http payload-length = 100000
```
http pdu-length

This command allows you to define rule expressions to match the total length of a single HTTP packet.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | http pdu-length operator pdu_length |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

pdu_length
Specifies the HTTP PDU length (in bytes) to match.
pdu_length must be an integer from 0 through 65535.

Usage Guidelines
Use this command to define rule expressions to match the total length of a single HTTP packet. This will also match packets with partial HTTP message (due to fragmentation).
Examples

The following command defines a rule expression to match an HTTP PDU length of 10000 bytes:

```
http pdu-length = 10000
```
**http previous-state**

This command allows you to define rule expressions to match previous state of HTTP sessions.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[no] http previous-state operator http_previous_state
```

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`operator`

Specifies how to match.

`operator` must be one of the following:

- `!=`: Does not equal
- `=`: Equals

`http_previous_state`

Specifies the previous state to match.

`http_previous_state` must be one of the following:

- `init`: Initialized state
- `response-error`: Response error state
- `response-ok`: Response ok state
- `waiting-for-response`: Waiting for response state
Usage Guidelines

Use this command to define rule expressions to match a previous state of HTTP sessions.

Examples

The following command defines a rule expression to match HTTP previous state `response-ok`:

```
http previous-state = response-ok
```
**http referer**

This command allows you to define rule expressions to match the value in the HTTP Referer request-header field.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

| no | http referer | case-sensitive | operator referer_name |

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  - Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `!contains`: Does not contain
    - `!ends-with`: Does not end with
    - `!present`: Not present
    - `!starts-with`: Does not start with
    - `=`: Equals
    - `contains`: Contains
    - `ends-with`: Ends with
**http referer**

- **present**: Present
- **regex**: Regular expression
- **starts-with**: Starts with

**referer_name**

Specifies the HTTP referer name to match.

**referer_name** must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

---

**Usage Guidelines**

Use this command to define rule expressions to match value in HTTP Referer request-header field.

This feature allows an operator to collect or track all URLs visited during a particular subscriber session. These URLs include the entire string of visited URLs, including all referral links. This information is output in an Event Data Record (EDR) format to support reporting or billing functions.

For example, if a subscriber begins a mobile web session and clicks on the "Sports" link from the home deck, and then selects ESPN and moves to an advertiser link, the operator can capture all URLs for that entire session. During this period ACS collects the URLs for a particular subscriber session; collection can be limited by time duration or number of URLs visited.

ACS generates EDRs that contain HTTP URL and the HTTP referer fields along with other fields.

In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the Enhanced Charging Service Administration Guide.

**Table 7: Special Characters Supported in Regex Rule Expressions**

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>?</td>
<td>Match zero or one character</td>
</tr>
</tbody>
</table>

**Important**

The CLI does not support configuring "?" directly, you must instead use "\077".

For example, if you want to match the string "xyz<any one character>pqr", you must configure it as:

**http host regex** "xyz\077pqr"

In another example, if you want to exactly match the string "url?resource=abc" , you must configure it as:

**http uri regex** "url\077resource=abc"

Where, the first \\ (backslash) is for the escaping of "?", and then "\077" for specifying "?" to the CLI.
### Regex Character

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>\</code> character</td>
<td>Escaped character</td>
</tr>
<tr>
<td><code>?</code></td>
<td>Match the question mark (<code>\&lt;ctrl-v&gt;</code>) character</td>
</tr>
<tr>
<td><code>+</code></td>
<td>Match the plus character</td>
</tr>
<tr>
<td><code>*</code></td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td><code>a</code></td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td><code>b</code></td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td><code>f</code></td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
<tr>
<td><code>n</code></td>
<td>Match the New line (ASCII 10) character</td>
</tr>
<tr>
<td><code>r</code></td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td><code>t</code></td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td><code>v</code></td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td><code>0</code></td>
<td>Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td><code>\</code></td>
<td>Match the backslash character</td>
</tr>
<tr>
<td>Bracketed range [0-9]</td>
<td>Match any single character from the range</td>
</tr>
<tr>
<td>A leading <code>^</code> in a range</td>
<td>Do not match any in the range. All other characters represent themselves.</td>
</tr>
<tr>
<td><code>\x##</code></td>
<td>Any ASCII character as specified in two-digit hex notation. For example, <code>\x5A</code> yields a &quot;Z&quot;.</td>
</tr>
</tbody>
</table>

|   | Specify OR regular expression operator |

**Important** When using the regex operator `|` in regex expressions, always wrap the string in double quotes. For example, if you want to match the string "pqr" OR "xyz", you must configure it as:

```
http host regex "pqr|xyz".
```

### Examples

The following command defines a rule expression to match the HTTP referer `cricket.espn.com`:

```
http referer = cricket.espn.com
```
http reply code

This command allows you to define rule expressions to match status code associated with HTTP response packets.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acsc-ruledef)#

Syntax Description

| no | http reply code operator reply_code

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

reply_code
Specifies the HTTP reply code to match.
reply_code must be an integer from 100 through 599.

Usage Guidelines
Use this command to define rule expressions to match status code associated with HTTP response codes.
Examples

The following command defines a rule expression to match HTTP response code 204:

```
http reply code = 204
```
http reply payload

This command allows you to define rule expressions to enable video detection using HTTP payload content.

Important
In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product
ACS
MVG

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name
Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description
| no | http reply payload type = video

no
If previously configured, deletes the specified rule expression from the current ruledef.

Usage Guidelines
Use this command to enable inspection for video in HTTP Response payload. Request payloads will not be inspected.
http request method

This command allows you to define rule expressions to match HTTP request method.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description

| no | http request method operator request_method |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- =: Equals

request_method
Specifies the HTTP request method to match.
request_method must be one of the following:

- connect
- delete
- get
- head
- options
http request method

- post
- put
- trace

**Usage Guidelines**

Use this command to define rule expressions to match an HTTP request method.

**Examples**

The following command defines a rule expression to match user traffic based on HTTP request method `connect`:

```
http request method = connect
```
**http session-length**

This command allows you to define rule expressions to match HTTP session length.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```text
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax Description**
```
| no | http session-length operator session_length |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **session_length**
  Specifies the HTTP total session length (in bytes) to match.
  
  `session_length` must be an integer from 1 through 4000000000.

**Usage Guidelines**
Use this command to define rule expressions to match a total HTTP session length.
The following command defines a rule expression to match an HTTP session length of 200000:

```
http session-length = 200000
```
http state

This command allows you to define rule expressions to match current state of an HTTP session.

**Product**    ACS

**Privilege**  Security Administrator, Administrator

**Command Modes**  Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**  

| no | http state operator current_state |

*no*

If previously configured, deletes the specified rule expression from the current ruledef.

*operator*

Specifies how to match.

*operator* must be one of the following:

- `!=`: Does not equal
- `=`: Equals

*current_state*

Specifies the current state of HTTP session to match.

*current_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 Guidelines**

Use this command to define rule expressions to match a current state of an HTTP session.

**Examples**

The following command defines a rule expression to match current state `close`:

```
http state = close
```
http transaction-length

This command allows you to define rule expressions to match HTTP transaction length (combined length of one HTTP GET Request message and its associated response messages).

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
| no | http transaction-length { operator transaction_length | { range | !range } range_from to range_to }

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• >=: Greater than or equals

transaction_length
Specifies the HTTP transaction length (in bytes) to match.
transaction_length must be an integer from 1 through 4000000000.

{ range | !range } range_from to range_to
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 Guidelines**
Use this command to define rule expressions to match an HTTP transaction length [one HTTP GET Request message + associated response message(s)] in bytes.

**Examples**
The following command defines a rule expression to match an HTTP transaction length of 10200 bytes:

```
http transaction-length = 10200
```
http transfer-encoding

This command allows you to define rule expressions to match the value in HTTP Transfer-Encoding general-header field.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | http transfer-encoding | case-sensitive | operator transfer_encoding |
```

- **no**

  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**

  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**

  Specifies how to match.

  * **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
**transfer_encoding**

Specifies the HTTP transfer encoding to match.

**transfer_encoding** must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match the value in HTTP Transfer-Encoding general-header field.

In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

**Examples**

The following command defines a rule expression to match the value *chunked* in HTTP Transfer-Encoding general-header field:

```
http transfer-encoding = chunked
```
http uri

This command allows you to define rule expressions to match HTTP URI.

Product  ACS

Privilege  Security Administrator, Administrator

Command Modes  Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description  | no | http uri | case-sensitive | operator uri

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
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
- regex: Regular expression
• **starts-with**: Starts with

**uri**

Specifies the HTTP URI to match.

**uri** must be an alphanumeric string of 1 through 127 characters, and can contain punctuation characters, and excludes the "host" portion.

**Usage Guidelines**

Use this command to define rule expressions to match an HTTP URI, excluding the host portion.

The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the *Enhanced Charging Service Administration Guide*.

*Table 8: Special Characters Supported in Regex Rule Expressions*

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>?</td>
<td>Match zero or one character</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>The CLI does not support configuring &quot;?&quot; directly, you must instead use &quot;\077&quot;. For example, if you want to match the string &quot;xyz&lt;any one character&gt;pqr&quot;, you must configure it as: <strong>http host regex</strong> &quot;xyz\077pqr&quot;</td>
</tr>
<tr>
<td></td>
<td>In another example, if you want to exactly match the string &quot;url?resource=abc&quot;, you must configure it as: <strong>http uri regex</strong> &quot;url\077resource=abc&quot;</td>
</tr>
<tr>
<td>\character</td>
<td>Escaped character</td>
</tr>
<tr>
<td>?</td>
<td>Match the question mark (&lt;ctrl-v&gt;-?) character</td>
</tr>
<tr>
<td>+</td>
<td>Match the plus character</td>
</tr>
<tr>
<td>*</td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td>\a</td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td>\b</td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td>\f</td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
<tr>
<td>\n</td>
<td>Match the New line (ASCII 10) character</td>
</tr>
<tr>
<td>Regex Character</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>\r</td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td>\t</td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td>\v</td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td>\0</td>
<td>Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td>\</td>
<td>Match the backslash character</td>
</tr>
<tr>
<td>Bracketed range [0-9]</td>
<td>Match any single character from the range</td>
</tr>
<tr>
<td>A leading ^ in a range</td>
<td>Do not match any in the range. All other characters represent themselves.</td>
</tr>
<tr>
<td>\x##</td>
<td>Any ASCII character as specified in two-digit hex notation. For example, \x5A yields a &quot;Z&quot;.</td>
</tr>
</tbody>
</table>

|         | Specify OR regular expression operator |
|         | **Important** When using the regex operator "|" in regex expressions, always wrap the string in double quotes. For example, if you want to match the string "pqr" OR "xyz", you must configure it as: |
|         | http host regex "pqr|xyz". |

**Examples**

The following command defines a rule expression to match the HTTP URI string http://www.somehost.com:

```bash
http uri = http://www.somehost.com
```

The following command defines a regex rule expression to match either of the following or similar values in the HTTP URI string: http://server19.com/search?form=zip, http://server20.com/search?form=pdf

```bash
```
http url

This command allows you to define rule expressions to match HTTP URL.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description

| no | http url | case-sensitive | operator url |

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.

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
- regex: Regular expression
**starts-with:** Starts with

**url**

Specifies the HTTP URL to match.

`url` must be an alphanumeric string of 1 through 127 characters that 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 ":/".

```plaintext
Hypertext Transfer Protocol
GET / HTTP/1.1
Request 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
Connection: Keep-Alive
```

**Usage Guidelines**

Use this command to define rule expressions to match HTTP URL.

The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the *Enhanced Charging Service Administration Guide*.

**Table 9: Special Characters Supported in Regex Rule Expressions**

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>?</td>
<td>Match zero or one character</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>The CLI does not support configuring &quot;?&quot; directly, you must instead use &quot;\077&quot;.</td>
</tr>
<tr>
<td>For example, if you want to match the string &quot;xyz&lt;any one character&gt;pqr&quot; , you must configure it as:</td>
<td></td>
</tr>
<tr>
<td><strong>http host regex</strong> &quot;xyz\077pqr&quot;</td>
<td></td>
</tr>
<tr>
<td>In another example, if you want to exactly match the string &quot;url?resource=abc&quot; , you must configure it as:</td>
<td></td>
</tr>
<tr>
<td><strong>http uri regex</strong> &quot;url\077resource=abc&quot;</td>
<td></td>
</tr>
<tr>
<td>Where, the first &quot;&quot; (backslash) is for the escaping of &quot;?&quot;, and then &quot;\077&quot; for specifying &quot;?&quot; to the CLI.</td>
<td></td>
</tr>
<tr>
<td>\character</td>
<td>Escaped character</td>
</tr>
<tr>
<td>?</td>
<td>Match the question mark (&lt;ctrl-v&gt;?)) character</td>
</tr>
<tr>
<td>Regex Character</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>+</td>
<td>Match the plus character</td>
</tr>
<tr>
<td>*</td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td>\a</td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td>\b</td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td>\f</td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
<tr>
<td>\n</td>
<td>Match the New line (ASCII 10) character</td>
</tr>
<tr>
<td>\r</td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td>\t</td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td>\v</td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td>\0</td>
<td>Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td>\</td>
<td>Match the backslash character</td>
</tr>
</tbody>
</table>

Bracketed range [0-9] Match any single character from the range

A leading ^ in a range Do not match any in the range. All other characters represent themselves.

\x## Any ASCII character as specified in two-digit hex notation.  
For example, \x5A yields a "Z".

<table>
<thead>
<tr>
<th></th>
<th>Specify OR regular expression operator</th>
</tr>
</thead>
</table>
| | Important When using the regex operator "|" in regex expressions, always wrap the string in double quotes.  
For example, if you want to match the string "pqr" OR "xyz", you must configure it as:  
http host regex "pqr|xyz".

**Examples**

The following command defines a rule expression to match the HTTP URL http://rfc.ietf.org/rfc/rfc1738.txt:  
```
http url = http://rfc.ietf.org/rfc/rfc1738.txt
```

The following command defines a regex rule expression to match either of the following or similar values in the HTTP URL string: http://yahoo.com, http://www.yahoo.co.in, http://yahoo.com/news.  
```
http url regex "(http://|http://www).yahoo.(co.in|com)*"
```
http user-agent

This command allows you to define rule expressions to match the User-Agent request-header field of HTTP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:
```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**

```

[ no ] http user-agent | case-sensitive | operator user_agent
```

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**case-sensitive**
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

**operator**
Specifies how to match.

`operator` must be one of the following:

- `!=`: Does not equal
- `!contains`: Does not contain
- `!ends-with`: Does not end with
- `!present`: Not present
- `!starts-with`: Does not start with
- `=`: Equals
- `contains`: Contains
- `ends-with`: Ends with
- **present**: Present
- **starts-with**: Starts with

**user_agent**

Specifies the HTTP user agent value to match.

*user_agent* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match value in HTTP user-agent header field.

In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

**Examples**

The following command defines a rule expression to match *xyz.123* in HTTP user-agent header field:

```
http user-agent = xyz.123
```
http version

This command allows you to define rule expressions to match version information in HTTP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]<host_name>(config-acs-ruledef)#

Syntax Description


no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !present: Not present
• !starts-with: Does not start with
• ==: Equals
• contains: Contains
• ends-with: Ends with
• **present**: Present
  • **starts-with**: Starts with

**http_version**

Specifies this HTTP version value to match.

http_version must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match HTTP version.

**Examples**

The following command defines a rule expression to match HTTP version http4.2:

```
http version = http4.2
```
http x-header

This command allows you to define rule expressions to match specified field within extension-headers (x-headers).

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | http x-header field_name | case-sensitive | operator string |
```

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**field_name**
field_name must be an alphanumeric string of 1 through 31 characters.

**case-sensitive**
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

**operator**
Specifies how to match.

operator must be one of the following:

- `!=`: Does not equal
- `!contains`: Does not contain
- `!ends-with`: Does not end with
- `!present`: Not present
- `!starts-with`: Does not start with
string

Specifies the HTTP x-header value to match.

string must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage Guidelines

Use this command to define rule expressions to match specified fields within x-headers. The extension-header can be any header field not specified in RFCs.

All x-header fields must begin with "x-".

In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

Examples

The following command defines a rule expression to match the extension-header test_field for the value test_string:

```
http x-header test_field = test_string
```
**icmp any-match**

This command allows you to define rule expressions to match all ICMP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] icmp any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  ```
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals
  ```

- **condition**
  Specifies the condition to match.
  ```
  condition must be one of the following:
  - FALSE
  - TRUE
  ```

**Usage Guidelines**
Use this command to define rule expressions to match all ICMP packets.
Examples

The following command defines a rule expression to match all ICMP packets:

```
icmp any-match = TRUE
```
**icmp code**

This command allows you to define rule expressions to match value in the Code field of ICMP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | icmp code operator code |
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**operator** must be one of the following:

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `=`: Equals
- `>=`: Greater than or equals

**code**

Specifies the ICMP code to match.

**code** must be an integer from 0 through 255.

**Usage Guidelines**

Use this command to define rule expressions to match a code field of ICMP packets.
Examples

The following command defines a rule expression to match ICMP code 11:

```
icmp code = 11
```
**icmp type**

This command allows you to define rule expressions to match value in Type field of ICMP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | icmp type operator type
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `<=`: Lesser than or equals
    - `=`: Equals
    - `>=`: Greater than or equals

- **type**
  Specifies the ICMP type to match.
  - `type` must be an integer from 0 through 255. For example, 0 for Echo Reply, 3 for Destination Unreachable, and 5 for Redirect.

**Usage Guidelines**
Use this command to define rule expressions to match a type field of ICMP packets.
**Examples**

The following command defines a rule expression to match user traffic based on ICMP type 3:

```
icmp type = 3
```
**icmpv6 any-match**

This command allows you to define rule expressions to match all ICMPv6 packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

**active-charging service service_name > ruledef ruledef_name**

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef) #

**Syntax Description**

| no | icmpv6 any-match operator condition |

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- !=: Does not equal
- ==: Equals

**condition**

Specifies the condition to match.

*condition* must be one of the following:

- FALSE
- TRUE

**Usage Guidelines**

Use this command to define rule expressions to match all ICMPv6 packets.
The following command defines a rule expression to match all ICMPv6 packets:

```plaintext
icmpv6 any-match = TRUE
```
icmpv6 code

This command allows you to define rule expressions to match value in Code field of ICMPv6 packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef)#

**Syntax Description**

| no | icmpv6 code operator code |

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

*operator* must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- =>: Greater than or equals

**code**
Specifies the ICMPv6 code to match.

*code* must be an integer from 0 through 255.

**Usage Guidelines**

Use this command to define rule expressions to match a code field of ICMPv6 packets.
Examples

The following command defines a rule expression to match ICMPv6 code 134:

```
icmpv6 code = 134
```
**icmpv6 type**

This command allows you to define rule expressions to match type field of ICMPv6 packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef)#

**Syntax Description**

`[no] icmpv6 type operator type`

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.
  
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- **type**
  
  Specifies the ICMPv6 type to match.
  
  `type` must be an integer from 0 through 255. For example, 129 for Echo Reply, 3 for Time Exceeded, and 137 for Redirect Message.

**Usage Guidelines**

Use this command to define rule expressions to match type field of ICMPv6 packets.
The following command defines a rule expression to match ICMPv6 type 133:

```
icmpv6 type = 133
```
if-protocol

This command allows you to associate different content IDs with the same ruledef, depending on the protocol being used.

Important

In StarOS 18.0 and later releases, this command has been deprecated.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

if-protocol { http | wsp-connection-less | wsp-connection-oriented } content-id content_id
no if-protocol { http | wsp-connection-less | wsp-connection-oriented }

no
If previously configured, deletes the specified rule expression from the current ruledef.

http
Specifies HTTP protocol.
This is the same as the rule expression http any-match = true.

wsp-connection-less
Specifies WSP connection-less protocol.
This is the same as requiring "wsp any-match = true" but "wtp any-match = false" (that is, connection-less WAP1.x).

wsp-connection-oriented
Specifies WSP connection-oriented protocol.
This is the same as the combined rule expression "\texttt{wsp any-match = true}" and "\texttt{wtp any-match = true}" (that is, connection-oriented WAP1.x).

\textbf{content-id content_id}

Specifies the content ID for the specified protocol.

In 12.1 and earlier releases, \textit{content_id} must be an integer from 1 through 65535.

In 12.2 and later releases, \textit{content_id} must be an integer from 1 through 2147483647.

\textbf{Usage Guidelines}

Use this command to associate different content IDs with the same ruledef, depending on the protocol being used.

This command is only effective for charging ruledefs. See the command for information on how to configure charging ruledefs.

If a particular ruledef should have three different values for content-id, depending on whether the traffic is connection-oriented WAP1.x, connection-less WAP1.x, or WAP2.0, within the ruledef we should have configuration similar to the following:

\begin{verbatim}
if-protocol wsp-connection-oriented content-id 1
if-protocol wsp-connection-less content-id 2
if-protocol http content-id 3
\end{verbatim}

Presumably, the ruledef would have another configurable like \texttt{www url contains foo}, which would cause it to use different content IDs when "foo" was accessed, depending upon the protocol being used.

\textbf{Examples}

The following command associates HTTP protocol and a content ID of 23:

\begin{verbatim}
if-protocol http content-id 23
\end{verbatim}
imap any-match

This command allows you to define rule expressions to match all IMAP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

```
[no] imap any-match operator condition
```

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

```
operator must be one of the following:

• !=: Does not equal
• ==: Equals
```

**condition**
Specifies the condition to match.

```
condition must be one of the following:

• FALSE
• TRUE
```

**Usage Guidelines**
Use this command to define rule expressions to match all IMAP packets.
The following command defines a rule expression to match all IMAP packets:

```
imap any-match = TRUE
```
**imap cc**

This command allows you to define rule expressions to match recipient address in the Carbon Copy (cc) field of e-mails in IMAP messages.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

**active-charging service service_name > ruledef ruledef_name**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

`[no] imap cc [case-sensitive] [operator cc_address]`

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  
  Specifies how to match.

  `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 e-mail "cc" address/name to match.

*cc_address* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match recipient address in the "cc" field of e-mails in IMAP messages.

**Examples**

The following command defines a rule expression to match recipient address *triangle@xyz.com* in the "cc" field of e-mails in IMAP messages:

```
imap cc contains triangle@xyz.com
```
imap command

This command allows you to define rule expressions to match embedded IMAP commands in IMAP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | imap command operator command |

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• ==: Equals

command

Specifies the command to match.

command must be one of the following:

• append
• authenticate
• capability
• check
• close
• copy
• create
• delete
• examine
• expunge
• fetch
• list
• login
• logout
• lsub
• noop
• rename
• search
• select
• starttls
• status
• store
• subscribe
• uid-copy
• uid-fetch
• uid-search
• uid-store
• unsubscribe

**Usage Guidelines**

Use this command to define rule expressions to match an embedded command in the IMAP message.

**Examples**

The following command defines a rule expression to match `close` command in IMAP messages:

`imap command = close`
imap content class

This command allows you to define rule expressions to match the content-class field of e-mails in IMAP messages.

**Product**  ACS

**Privilege**  Security Administrator, Administrator

**Command Modes**  Exec > ACS Configuration > Ruledef Configuration

```
active-chargingservice service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>no</th>
<th>imap content class</th>
<th>case-sensitive</th>
<th>operator content_class</th>
</tr>
</thead>
</table>

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**case-sensitive**

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

**operator**

Specifies how to match.

`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 content class to match.

(content_class) must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage Guidelines

Use this command to define rule expressions to match the content-class field of e-mails in IMAP messages.

Examples

The following command defines a rule expression to analyze user traffic matching content class javax.mail.internet.MimeMultipart in the content-class field of e-mails in IMAP messages:

imap content class contains javax.mail.internet.MimeMultipart
**imap content type**

This command allows you to define rule expressions to match the content-type field of e-mails in IMAP messages.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

| no | imap content type | case-sensitive | operator content_type |

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  **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 content type field to match.

*content_type* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match the content-type field of e-mails in IMAP messages.

**Examples**

The following command defines a rule expression to analyze user traffic matching content type `TEXT/plain; charset=iso-8859-1` in the content-type field of e-mails in IMAP messages:

```
imap content type contains TEXT/plain; charset=iso-8859-1
```
imap date

This command allows you to define rule expressions to match the Date field of e-mails in IMAP messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | imap date | case-sensitive | operator date |

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  - **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 date to match.

date must be an alphanumeric string of 1 through 127 characters that may include punctuation marks and spaces as shown in the example below.

**Usage Guidelines**

Use this command to define rule expressions to match the date field of e-mails in IMAP messages.

**Examples**

The following command defines a rule expression to analyze user traffic matching date *Fri, 20 Jan 2012 11:00:00 -0600* in the "date" field of e-mails in IMAP messages:

imap date contains Fri, 21 Jan 2012 11:00:00 -0600
imap final-reply

This command allows you to define rule expressions to match final-reply value for the last IMAP final-reply message.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:
```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**

`| no | imap final-reply operator final_reply`

- **no**  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**  
  Specifies how to match.  
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **final_reply**  
  Specifies the "final-reply" condition to match.  
  `final_reply` 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 Guidelines

Use this command to define rule expressions to match a final-reply value for the last IMAP final-reply message.

Examples

The following command defines a rule expression to analyze user traffic matching the final-reply condition `bad` in the last IMAP final-reply message:

```
imap final-reply = bad
```
imap from

This command allows you to define rule expressions to match the from field of e-mails in IMAP messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
``` 

**Syntax Description**

```
| no | imap from | case-sensitive | operator from_address |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  
  `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_address
Specifies the "from" address/value to match.
from_address must be an alphanumerical string of 1 through 127 characters.

Usage Guidelines
Use this command to define rule expressions to match the from field of e-mails in IMAP messages.

Examples
The following command defines a rule expression to analyze user traffic matching triangle in the "from" field of e-mails in the IMAP messages:
imap from contains triangle
imap mail-size

This command allows you to define rule expressions to match IMAP e-mail users that have e-mails of a specified size in their mailboxes.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**
[no] imap mail-size operator mail_size

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

**operator** must be one of the following:
- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- =>: Greater than or equals

**mail_size**
Specifies the total size of mail, in bytes, to match.

**Usage Guidelines**
Use this command to define rule expressions to discover the number of IMAP e-mail users that have e-mails of a specified size in their mailboxes.
**Examples**

The following command defines a rule expression to match users with e-mail size less than or equal to 23400 bytes:

```
imap mail-size <= 23400
```
**imap mailbox-size**

This command allows you to define rule expressions to match IMAP e-mail user having a specified number of messages in their mailboxes.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

`| no | imap mailbox-size operator number_of_email`

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `==`: Equals
- `>=`: Greater than or equals

**number_of_email**

Specifies the total number of e-mail messages in mailbox of an IMAP user to match.

*number_of_email* must be an integer from 0 through 65535.

**Usage Guidelines**

Use this command to define rule expressions to match the number of IMAP e-mail users having a specified number of messages in their mailboxes.
The following command defines a rule expression to match e-mail users having less than or equal to 1024 e-mail messages in their mailboxes:

```
imap mailbox-size <= 1024
```
imap message-type

This command allows you to define rule expressions to match the type of IMAP packet.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration  

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax Description**

```
[ no ] imap message-type operator message_type
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**message_type**

Specifies the IMAP packet message-type to match.

- **command-continuation-reply**: Message with command-continuation-reply type.
- **final-reply**: Message is of final reply type.
- **request**: There is of request type.
- **untagged-reply**: Message of reply type, but without any tag.
**Usage Guidelines**

Use this command to define rule expressions to match the IMAP message type.

**Examples**

The following command defines a rule expression to match IMAP sessions with message type `request`:

```
imap message-type = request
```
imap previous-state

This command allows you to define rule expressions to match the previous state of IMAP request sessions.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description | no | imap previous-state operator imap_previous_state

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

- \(!=\): Does not equal
- \(=\): Equals

imap_previous_state

Specifies the previous state to match.

imap_previous_state must be one of the following:

- \(init\): Message in initialization state.
- \(request-sent\): Message in request-sent state.

Usage Guidelines Use this command to define rule expressions to match previous state of IMAP request session.
Examples

The following command defines a rule expression to match IMAP sessions with previous state **init**:

```
imap previous-state = init
```
imap session-length

This command allows you to define rule expressions to match the total length of an IMAP session.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] imap session-length operator session_length
```

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

`operator` must be one of the following:

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `=:` Equals
- `>=`: Greater than or equals

**session_length**
Specifies the total length of IMAP session (in bytes) to match.

`session_length` must be an integer from 1 through 400000000.

**Usage Guidelines**
Use this command to define rule expressions to match the total length of IMAP sessions.

The session length is calculated by adding together the IP payloads (that is, starting after the IP header) of all relevant IMAP session packets.
Examples

The following command defines a rule expression to match IMAP sessions with length less than or equal to 4000 bytes:

imap session-length <= 4000
**imap session-previous-state**

This command allows you to define rule expressions to match the previous state of an IMAP session.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service *service_name* > ruledef *ruledef_name*

Entering the above command sequence results in the following prompt:

[local] *host_name* (config-acs-ruledef) #

**Syntax Description**

[ no ] **imap session-previous-state** *operator* **imap_session_previous_state**

*no*

If previously configured, deletes the specified rule expression from the current ruledef.

*operator*

Specifies how to match.

*operator* must be one of the following:

- !=: Does not equal
- =: Equals

**imap_session_previous_state**

Specifies the previous state of IMAP session to match.

*imap_session_previous_state* must be one of the following:

- **authenticated**: Session authenticated
- **connected**: Session connected
- **init**: Session initialized
- **mailbox-selected**: Mailbox selected
Usage Guidelines

Use this command to define rule expressions to match the previous state of IMAP sessions.

Examples

The following command defines a rule expression to match IMAP sessions with previous state init:

`imap session-previous-state = init`
imap session-state

This command allows you to define rule expressions to match the current state of IMAP sessions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**
```plaintext
[ no ] imap session-state operator session_current_state
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.

  - `!=`: Does not equal
  - `=`: Equals

- **session_current_state**
  Specifies the current state to match.

  `session_current_state` must be one of the following:

  - **authenticated**: Session authenticating.
  - **connected**: Session connecting.
  - **logout**: Session logged out.
  - **mailbox-selected**: Mailbox selecting.
### Usage Guidelines

Use this command to define rule expressions to match the current state of IMAP sessions.

### Examples

The following command defines a rule expression to match IMAP sessions with current state `connected`:

```
imap session-state = connected
```
**imap state**

This command allows you to define rule expressions to match the current state of IMAP sessions.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```bash
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```bash
| no | imap state operator current_state
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  `operator` must be one of the following:

  - `!=`: Does not equal
  - `=`: Equals

- **current_state**
  
  Specifies current state of IMAP session to match.

  `current_state` must be one of the following:

  - `request-sent`: Request message sent
  - `response-fail`: Request response failed
  - `response-ok`: Request response is good

**Usage Guidelines**

Use this command to define rule expressions to match the current state of IMAP session.
The following command defines a rule expression to match IMAP sessions with current state `response-fail`:

```
imap state = response-fail
```
imap subject

This command allows you to define rule expressions to match the subject field of e-mails in IMAP messages.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef)#

Syntax Description

| no | imap subject | case-sensitive | operator subject |

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.

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 "subject" to match.

subject must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters and space as shown in the example below.

Usage Guidelines

Use this command to define rule expressions to match "subject" field of e-mail in IMAP message.

Examples

The following command defines rule expression to match occurrence of the string My test in the "subject" field of e-mails in IMAP message:

imap subject contains My test
imap to

This command allows you to define rule expressions to match the "to" field of e-mails in IMAP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef)#

Syntax Description

| no | imap to | case-sensitive | operator to |

  no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.

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 "to" field value to match.

To must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage Guidelines

Use this command to define rule expressions to match "to" field of e-mails in IMAP messages.

Examples

The following command defines a rule expression to analyze user traffic matching the occurrence xyz.com in the "to" field of e-mails in the IMAP message:

`imap to contains xyz.com`
**ip any-match**

This command allows you to define rule expressions to match all IPv4/IPv6 packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] ip any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage Guidelines**

Use this command to define rule expressions to match IPv4/IPv6 packets.
Examples

The following command defines a rule expression to match IPv4/IPv6 packets:

```
ip any-match = TRUE
```
**ip dscp**

This command enables you to configure a ruledef with the DSCP value and match it with the DSCP value in the incoming IP packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**

```
[ no ] ip dscp { operator } ipv4_tos_value | ipv6_tc_value [ mask mask_value ]
```

*no*

If previously configured, removes the specified DSCP value and the mask from the configuration.

*operator*

Specifies how to match.

*operator* must be one of the following:

- !: Does not equal
- =: Equals

*ipv4_tos_value | ipv6_tc_value*

Specifies the DSCP value to match with the incoming IP packets.

The *ipv4_tos_value* or *ipv6_tc_value* must be an integer from 0 through 63.

*mask mask_value*

Specifies the mask for the number of bits in the DSCP value to be considered for matching.

*mask_value* must be an integer from 0 through 63. The default mask value is 63.
Usage Guidelines

Use this command to check if the DSCP value in the IPv4 ToS or IPv6 TC field of incoming IP packet matches with configured ToS/TC value.

Examples

The following command will match all incoming packets which has DSCP value 20:

```
ip dscp = 20 mask 31
```
**ip downlink**

This command allows you to define rule expressions to match downlink (network to subscriber) packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] ip downlink operator condition
```

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`operator`

Specifies how to match.

`operator` must be one of the following:

- `!=`: Does not equal
- `==`: Equals

`condition`

Specifies the condition to match.

`condition` must be one of the following:

- `FALSE`
- `TRUE`

**Usage Guidelines**

Use this command to define rule expressions to match downlink (to subscriber) IP packets.
Examples

The following command defines a rule expression to match IP packet in downlink direction:

`ip downlink = TRUE`
ip dst-address

This command allows you to define rule expressions to match IP destination address field within IP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no | ip dst-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask | address-group ipv6_address } | { !range | range } host-pool host_pool_name }]
```

*no*
If previously configured, deletes the specified rule expression from the current ruledef.

*operator*
*operator*: Specifies how to match.

*operator* must be one of the following:

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `=`: Equals
- `>=`: Greater than or equals

*ipv4/ipv6_address*
Specifies the IP address of the destination node for outgoing traffic. *ipv4/ipv6_address* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
ipv4/ipv6_address/mask

Specifies the IP address of the destination node for outgoing traffic. `ipv4/ipv6_address/mask` must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which corresponding to the number of bits in the subnet mask.

address-group ipv6_address

The `address-group` keyword can be configured only after the `=` operator. The wildcard support has not been provided for IPv4 addresses.

**Important**

Specifies a group of IPv6 addresses configured with wildcard input and/or specialized range input. Multiple wildcard characters can be accepted as input and only one 2 byte range input will be accepted. Both wildcard character input and 2 byte range input can be configured together within a given IPv6 address.

In the example — `2607:7700:*:[2020-3040]:::ce1d:b083/128`, * is a wildcard input and `[2020-3040]` is a 2 byte specialized range input.

{ !range | range } host-pool host_pool_name

!range | range: Specifies the range criteria:

- !range: Not in the range of
- range: In the range of

host-pool host_pool_name: Specifies the name of the host pool. `host_pool_name` must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to define rule expressions to match the IP destination address field within IP headers.

**Examples**

The following command defines a rule expression to match user traffic based on the IPv4 destination address `10.1.1.1`:

```
ip dst-address = 10.1.1.1
```

The following command defines a rule expression to match user traffic based on the given destination IPv6 address where * is the wildcard input and `[2020-3040]` is the 2 byte specialized range input:

```
ip dst-address = 2607:7700:*:[2020-3040]:::ce1d:b083/128
```
ip error

This command allows you to define rule expressions to match user traffic for invalid IP packets and other errors, for example IP header error, while parsing IP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] ip error operator condition
```

*no*
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

`operator` must be one of the following:

- `!=`: Does not equal
- `=`: Equals

**condition**
Specifies the condition to match.

`condition` must be one of the following:

- `FALSE`
- `TRUE`

**Usage Guidelines**
Use this command to define rule expressions to match invalid IP packets and any other errors while parsing IP packets.
Examples

The following command defines a rule expression to match user traffic for invalid IP packets and other errors:

```
ip error = TRUE
```
**ip protocol**

This command allows you to define rule expressions to match the protocol field in IP headers.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration  
*active-charging service service_name > ruledef ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**  
```
[ no ] ip protocol operator { protocol_assignment_no | protocol }
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  
  **operator** must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals—available only in 8.1 and later releases
  - `=`: Equals
  - `>=`: Greater than or equals—available only in 8.1 and later releases

- **protocol_assignment_no**
  Specifies the protocol by assignment number.
  
  **protocol_assignment_no** 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 Guidelines

Use this command to define rule expressions to match protocol field in IP packet headers.

Examples

The following command defines a rule expression to match protocol assignment number 1:

```
ip protocol = 1
```
ip server-domain-name

This command allows you to define rule expressions to match host names (domain names).

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | ip server-domain-name operator domain_name |

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- *=: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

**domain_name**

Specifies the domain name to match.

*domain_name* must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to define rule expressions to match full or partial host names (domain names).

The rule will be matched for the learnt IP addresses resolved from DNS queries to the specified domain names.

DNS responses for the specified domain names will be snooped and the learnt IP addresses stored.
Besides being used for standard rule matching, this command also enables the DNS Snooping feature if the rulebase references any ruledefs with this configuration. The DNS protocol analyzer must also be enabled in the rulebase.

**Examples**

The following command defines a rule expression to match domain name values containing *star*:

```
ip server-domain-name contains star
```
**ip server-ip-address**

This command allows you to define rule expressions to match the IP address of the destination end of the connection.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

```
| no | ip server-ip-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask | address-group ipv6_address } | { !range | range } host-pool host_pool_name }
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  **operator** must be one of the following:
  - !=: Does not equal
  - <=: Lesser than or equals
  - ==: Equals
  - >=: Greater than or equals

- **ipv4/ipv6_address**
  Specifies the server IP address. For uplink packets (subscriber to network), this field matches the destination IP address in the IP header. For downlink packets (network to subscriber), this field matches the source IP address in the IP header. **ipv4/ipv6_address** must be an IP address in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.
**ipv4/ipv6_address/mask**

Specifies the server IP address with subnet mask bit. For uplink packets (subscriber to network), this field matches the destination IP address in the IP header. For downlink packets (network to subscriber), this field matches the source IP address in the IP header. *ipv4/ipv6_address/mask* must be an IP address in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.

**address-group ipv6_address**

**Important**

The **address-group** keyword can be configured only after the = operator. The wildcard support has not been provided for IPv4 addresses.

Specifies a group of IPv6 addresses configured with wildcard input and/or specialized range input. Multiple wildcard characters can be accepted as input and only one 2 byte range input will be accepted. Both wildcard character input and 2 byte range input can be configured together within a given IPv6 address.

In the example — `2607:7700:*:[2020-3040]::ce1d:b083/128`, * is a wildcard input and [2020-3040] is a 2 byte specialized range input.

```{!range | range} host-pool host_pool_name```

!range | range: Specifies the range criteria:

- !range: Not in the range of
- range: In the range of

host-pool host_pool_name: Specifies name of the host pool. *host_pool_name* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to define rule expressions to match the IP address of the destination end of the connection. For uplink packets, this field matches the destination IP address in the IP header. For downlink packets, this field matches the source IP address in the IP header.

**Examples**

The following command defines a rule expression to match user traffic based on IPv4 server address `10.1.1.1`:

```
   ip server-ip-address = 10.1.1.1
```

The following command defines a rule expression to match user traffic based on the given destination IPv6 address where * is the wildcard input and [2020-3040] is the 2 byte specialized range input:

```
   ip server-ip-address = 2607:7700:*:[2020-3040]::ce1d:b083/128
```
ip src-address

This command allows you to define rule expressions to match the source IP address field within IP headers.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

\[ \text{no} \mid \text{ip src-address} \{ \text{operator} \{ \text{ipv4/ipv6\_address} | \text{ipv4/ipv6\_address/mask} | \text{address\_group} \text{ipv6\_address} \} \mid \{ \text{!range} | \text{range} \} \text{host\_pool host\_pool\_name} \}\]

\text{no}

If previously configured, deletes the specified rule expression from the current ruledef.

\text{operator}

\text{operator} \text{ specifies how to match.}

\text{operator} \text{ must be one of the following:}

- \text{!=}: Does not equal
- \text{<=}: Lesser than or equals
- \text{=} : Equals
- \text{>=}: Greater than or equals

\text{ipv4/ipv6\_address}

Specifies IP address of the source node for incoming traffic. \text{ipv4/ipv6\_address} \text{ must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.}
**ipv4/ipv6_address/mask**

Specifies the IP address of the source node for incoming traffic with subnet mask bit. `ipv4/ipv6_address/mask` must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which corresponds to the number of bits in the subnet mask.

**address-group ipv6_address**

---

**Important**

The `address-group` keyword can be configured only after the `=` operator. The wildcard support has not been provided for IPv4 addresses.

**Important**

Specifies a group of IPv6 addresses configured with wildcard input and/or specialized range input. Multiple wildcard characters can be accepted as input and only one 2 byte range input will be accepted. Both wildcard character input and 2 byte range input can be configured together within a given IPv6 address.

In the example — `2607:7700:*:[2020-3040]::ce1d:b083/128`, * is a wildcard input and [2020-3040] is a 2 byte specialized range input.

---

---

**{ !range | range } host-pool host_pool_name**

- **!range**: Specifies the range criteria:
  - **!range**: Not in the range of
  - **range**: In the range of

**host-pool host_pool_name**: Specifies name of the host pool. `host_pool_name` must be a string of 1 through 63 characters.

---

**Usage Guidelines**

Use this command to define rule expressions to match IP source address field within IP header.

---

**Examples**

The following command defines a rule expression to match user traffic based on IPv4 source address `10.1.1.1`:

```
ip src-address = 10.1.1.1
```

The following command defines a rule expression to match user traffic based on the given source IPv6 address where * is the wildcard input and [2020-3040] is the 2 byte specialized range input:

```
ip src-address = 2607:7700:*:[2020-3040]::ce1d:b083/128
```
### ip subscriber-ip-address

This command allows you to define rule expressions to match the IP address of the subscriber, which will be either the source or destination address depending on the direction.

#### Product

ACS

#### Privilege

Security Administrator, Administrator

#### Command Modes

Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef) #
```

#### Syntax Description

```plaintext
| no | ip subscriber-ip-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask | address-group ipv6_address } | { !range | range } host-pool host_pool_name }
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

*operator*: Specifies how to match.

*operator* must be one of the following:

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `=`: Equals
- `>=`: Greater than or equals

**ipv4/ipv6_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. *ipv4/ipv6_address* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
**ipv4/ipv6_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. *ipv4/ipv6_address/mask* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which corresponds to the number of bits in the subnet mask.

**address-group ipv6_address**

---

**Important**
The *address-group* keyword can be configured only after the = operator. The wildcard support has not been provided for IPv4 addresses.

---

Specifies a group of IPv6 addresses configured with wildcard input and/or specialized range input. Multiple wildcard characters can be accepted as input and only one 2 byte range input will be accepted. Both wildcard character input and 2 byte range input can be configured together within a given IPv6 address.

In the example — *2607:7700:*:[2020-3040]::ce1d:b083/128*, * is a wildcard input and [2020-3040] is a 2 byte specialized range input.

---

**{ !range | range } host-pool host_pool_name**

* !range | range: Specifies the range criteria:
  • !range: Not in the range of
  • range: In the range of

*host-pool host_pool_name*: Specifies the name of the host pool. *host_pool_name* must be an alphanumeric string of 1 through 63 characters.

---

**Usage Guidelines**

Use this command to define rule expressions to match the IP address of the subscriber, which will be either the source or destination address depending on the direction.

---

**Examples**

The following command defines a rule expression to match user traffic based on subscriber IPv4 address 10.1.1.1:

```
ip subscriber-ip-address = 10.1.1.1
```

The following command defines a rule expression to match user traffic based on the given subscriber IPv6 address where * is the wildcard input and [2020-3040] is the 2 byte specialized range input:

```
ip subscriber-ip-address = 2607:7700:*:[2020-3040]::ce1d:b083/128
```
ip total-length

This command allows you to define rule expressions to match the total length field in IP headers.

Product ACS

Privilege Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef) #

Syntax Description

| no | ip total-length operator total_length

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• >=: Greater than or equals

total_length
Specifies the total length of the IP packet (including payload) to match.
total_length must be an integer from 0 through 4096.

Usage Guidelines
Use this command to define rule expressions to match the total length field in IP headers.
**Examples**

The following command defines a rule expression to match user traffic based on IP total length of 2000 bytes:

```plaintext
ip total-length = 2000
```
**ip uplink**

This command allows you to define rule expressions to match uplink (subscriber to network) IP packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | ip uplink operator condition
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**

  Specifies how to match.

  - **operator** must be one of the following:
    - `!`: Does not equal
    - `=`: Equals

- **condition**

  Specifies the condition to match.

  - **condition** must be one of the following:
    - `FALSE`
    - `TRUE`

**Usage Guidelines**

Use this command to define rule expressions to match uplink (subscriber to network) IP packets.
Examples

The following command defines a rule expression to match uplink packets:

```
ip uplink = TRUE
```
ip version

This command allows you to define rule expressions to match the version number in IP headers.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
[no ] ip version operator ip_version

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be = (equals).

ip_version
Specifies the IP version to match.
ip_version must be one of the following:
- ipv4
- ipv6

Usage Guidelines
Use this command to define rule expressions to match version number in IP header.

Examples
The following command defines a rule expression to match user traffic for the IP version ipv6:
ip version = ipv6
mms any-match

This command allows you to define rule expressions to match all Multimedia Messaging Service (MMS) packets.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration

```active-chargingservice service_name > ruledef ruledef_name```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**  
```
no | mms any-match operator condition
```

*no*

If previously configured, deletes the specified rule expression from the current ruledef.

*operator*

Specifies how to match.

*operator* must be one of the following:

- !=: Does not equal
- ==: Equals

*condition*

Specifies the condition to match.

*condition* must be one of the following:

- FALSE
- TRUE

**Usage Guidelines**  
Use this command to define rule expressions to match all MMS packets.
The following command defines a rule expression to match all MMS packets:

```
mms any-match = TRUE
```
mms bcc

This command allows you to define rule expressions to match recipient addresses in the bcc field of MMS messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | mms bcc | case-sensitive | operator bcc_address |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  **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
**Usage Guidelines**
Use this command to define rule expressions to match recipient address in the "bcc" field of MMS messages.

**Examples**
The following command defines a rule expression to match recipient address containing `test1` in "bcc" field of MMS messages:

```plaintext
mms bcc contains test1
```
mms cc

This command allows you to define rule expressions to match recipient addresses in the cc field of MMS messages.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]\host_name(config-acs-ruledef)#

**Syntax Description**

| no | mms cc | case-sensitive | operator cc_address |

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**case-sensitive**

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

**operator**

Specifies how to match.

* 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 "cc" address/value to match.

*cc_address* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.

**Usage Guidelines**

Use this command to define rule expressions to match recipient addresses in "cc" field of MMS messages.

**Examples**

The following command defines a rule expression to match recipient address containing *test1* in the "cc" field of MMS messages:

```plaintext
mms cc contains test1
```
**mms content location**

This command allows you to define rule expressions to match the content-location field of MMS messages.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**  

```plaintext
| no | mms content location | case-sensitive | operator string
```

- **no**  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**  
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**  
  Specifies how to match.

  * **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 to match.

*string* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.

**Usage Guidelines**

Use this command to define rule expressions to match the content-location field of MMS messages.

**Examples**

The following command defines a rule expression to match *test1* in content-location field of MMS messages:

```
mms content location contains test1
```
**mms content type**

This command allows you to define rule expressions to match the content-type field of MMS messages.

**Product** ACS

**Privilege** Security Administrator, Administrator

**Command Modes**

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | mms content type | case-sensitive | operator content_type |
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  - Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  - Specifies how to match.
  - **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 MMS content type to match.

*content_type* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.

**Usage Guidelines**

Use this command to define rule expressions to match content-type field of MMS messages.

**Examples**

The following command defines a rule expression to match *image* in content-type field of MMS messages:

```
mms content type contains image
```
**mms downlink**

This command allows you to define rule expressions to match downlink (network to subscriber) MMS packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**

```
[ no ] mms downlink operator condition
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**condition**

Specifies the downlink (from the Mobile Node direction) status to match.

**Usage Guidelines**

Use this command to define rule expressions to match downlink MMS packets.
Examples

The following command defines a rule expression to match all downlink MMS packets:

\texttt{mms downlink = TRUE}
mms from

This command allows you to define rule expressions to match the "from" field in MMS messages.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs-ruledef) #

Syntax Description

| no | mms from | case-sensitive | operator from_address |

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
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
\textit{from_address}

Specifies the "from" address/value to match.

\textit{from_address} must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.

**Usage Guidelines**

Use this command to define rule expressions to match the "from" field of MMS messages.

**Examples**

The following command defines a rule expression to match \textit{test1} in the "from" field of MMS messages:

\texttt{mms from contains test1}
mms message-id

This command allows you to define rule expressions to match the message ID field of MMS messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**
```
| no | mms message-id | case-sensitive | operator message_id |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  - **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
message_id

Specifies the MMS message ID to match.

message_id must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage Guidelines

Use this command to define rule expressions to match the "message ID" field of MMS messages.

Examples

The following command defines a rule expression to match test1 in the "message ID" field of MMS messages:

```
mms message-id contains test1
```
mms pdu-type

This command allows you to define rule expressions to match Protocol Data Unit (PDU) type in the current MMS packets.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description
| no | mms pdu-type operator pdu_type |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• ==: Equals

pdu_type
Specifies the MMS PDU type to match.
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-response**: This option is deprecated. Use the `mms_pdu_type_m_retrieve_conf` option instead.

**Usage Guidelines**

Use this command to define rule expressions to match the PDU type in the current MMS packet.

**Examples**

The following command defines a rule expression to match PDU type `mms-pdu-type-m-http-get` in the current MMS packet:

```
mms pdu-type = mms-pdu-type-m-http-get
```
**mms previous-state**

This command allows you to define rule expressions to match the previous state of MMS sessions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | mms previous-state operator mss_previous_state
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**operator** must be one of the following:

* !=: Does not equal
* ==: Equals

**mms_previous_state**

Specifies the previous state to match.

**mms_previous_state** must be one of the following:

* delayed-ack-pending: This option is deprecated, use retrieve-conf-received.
* delayed-m-notify-rsp-sent: This option is deprecated, use notify-rsp-sent.
* delayed-retrieval-pending: This option is deprecated, use retrieval-pending.
* immediate-retrieval-pending: This option is deprecated, use retrieval-pending.
* init
- m-send-conf-rcvd: This option is deprecated, use send-success.
- m-send-req-sent
- notification-ind-rcvd
- notify-rsp-sent
- retrieval-pending
- retrieve-conf-received
- send-success

**Usage Guidelines**

Use this command to define rule expressions to match the previous state of MMS sessions.

**Examples**

The following command defines a rule expression to match user traffic based on MMS previous state of retrieval-pending:

```
mms previous-state = retrieval-pending
```
**mms response status**

This command allows you to define rule expressions to match the response status code of MMS messages.

**Product** ACS

**Privilege** Security Administrator, Administrator

**Command Modes**

```
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | mms response status operator status_code
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  - **operator** must be one of the following:
    - `!=`: Does not equal
    - `=`: Equals

- **status_code**
  
  Specifies the status code to match.

  `status_code` must be an integer from 128 through 136.

**Usage Guidelines**

Use this command to define rule expressions to match response status code of MMS messages.

**Examples**

The following command defines a rule expression to match user traffic based on MMS response status code 129:

```
mms response status = 129
```
**mms state**

This command allows you to define rule expressions to match the current state of MMS sessions.

**Product** ACS

**Privilege** Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef)#

**Syntax Description**

| no | mms state operator current_state |

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

 Specifies how to match.

*operator* must be one of the following:

- !=: Does not equal
- :=: Equals

**current_state**

Specifies current state of MMS session to match.

*current_state* must be one of the following:

- delayed-ack-pending: This option is deprecated, use retrieve-conf-received.
- delayed-m-notify-rsp-sent: This option is deprecated, use notify-rsp-sent.
- delayed-retrieval-pending: This option is deprecated, use retrieval-pending.
- delivery-failed
- delivery-success
- **immediate-retrieval-pending**: This option is deprecated, use **retrieval-pending**.
- **m-send-conf-rcvd**: This option is deprecated, use **send-success**.
- **m-send-req-sent**
- **notification-ind-rcvd**
- **notify-rsp-sent**
- **retrieval-failed**
- **retrieval-pending**
- **retrieval-success**
- **retrieve-conf-received**
- **send-success**

**Usage Guidelines**

Use this command to define rule expressions to match the current state of MMS session.

**Examples**

The following command defines a rule expression to match user traffic based on the current state of MMS session as **retrieval-failed**:

```
mms state = retrieval-failed
```
**mms status**

This command allows you to define rule expressions to match the current status of MMS sessions.

**Product** ACS

**Privilege** Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] mms status operator status
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `=`: Equals

- **status**
  - Specifies the MMS status to match.
  - `status` must be an integer from 128 through 132.

**Usage Guidelines**

Use this command to define rule expressions to match current status of MMS sessions.

**Examples**

The following command defines a rule expression to match user traffic based on MMS current status 130:

```
mms status = 130
```
mms subject

This command allows you to define rule expressions to match the "subject" field of MMS messages.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
| no | mms subject | case-sensitive | operator subject_string |

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
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_string

Specifies the value to match.

*subject_string* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.

**Usage Guidelines**

Use this command to define rule expressions to match "subject" field of MMS messages.

**Examples**

The following command defines a rule expression to match *test1* in the "subject" field of MMS messages:

```
mmssubject contains test1
```
**mms tid**

This command allows you to define rule expressions to match the "Transaction Identifier" (TID) field of MMS messages.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | mms tid | case-sensitive | operator transaction_id |

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

**Operator**

Specifies how to match.

*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
**transaction_id**

Specifies the MMS TID to match.

*transaction_id* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match TID field of MMS messages.

**Examples**

The following command defines a rule expression to match *test* in TID field of MMS messages:

```
mms tid = test
```
**mms to**

This command allows you to define rule expressions to match the "to" field of MMS messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | mms to | case-sensitive | operator to_address
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  
  Specifies how to match.

  `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_address

Specifies the "to" address/name to match.

to_address must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters and space.

Usage Guidelines

Use this command to define rule expressions to match "to" field of MMS messages.

Examples

The following command defines a rule expression to match user traffic based on test in "to" field of MMS messages:

```plaintext
mms to = test
```
**mms uplink**

This command allows you to define rule expressions to match uplink (subscriber to network) MMS packets.

**Product**
- ACS

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec
- ACS Configuration
- Ruledef Configuration

**Syntax Description**

```
[no] mms uplink [operator] condition
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
    - **operator** must be one of the following:
      - `!=`: Does not equal
      - `=`: Equals

- **condition**
  - Specifies the uplink (from the Mobile Node direction) status to match.
    - **condition** must one of the following:
      - `FALSE`
      - `TRUE`

**Usage Guidelines**
- Use this command to define rule expressions to match uplink MMS packets.
Examples

The following command defines a rule expression to match uplink MMS packets:

```plaintext
mms uplink = TRUE
```
mms version

This command allows you to define rule expressions to match the MMS version in MMS packets.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | mms version operator version |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• ==: Equals

version
Specifies the MMS version to match.

version must be an integer from 1 through 65535.

Important
MMS protocol analyzer supports decoding of only MMS version 1.0.

Usage Guidelines
Use this command to define rule expressions to match MMS version in MMS packets.
Examples

The following command defines a rule expression to match MMS version 1.0 in MMS packets:

```
mms version = 1
```
multi-line-or all-lines

This command applies the OR operator to all lines in the current ruledef.

Product ACS

Privilege Security Administrator, Administrator

Command Modes

- Exec > ACS Configuration > Ruledef Configuration
- active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | multi-line-or all-lines |

no
If previously configured, deletes this configuration in the current ruledef.

multi-line-or all-lines
Applies the OR operator to all lines in the current ruledef.

Usage Guidelines

When a ruledef is evaluated, if the multi-line-or all-lines command is configured, the logical OR operator is applied to all the rule expressions in the ruledef to decide if the ruledef matches or not. If the multi-line-or all-lines command is not configured, the logical AND operator is applied to all the rule expressions.

The intent of this command is to allow a single ruledef to specify multiple URL expressions. Otherwise, multiple ruledefs need to be created, each with one URL expression. When this CLI command is used, each expression in the ruledef impacts the total number of ruledefs allowed. So from a "maximum number of possible rules" perspective, it makes no difference whether there are N ruledefs with one expression each, or one ruledef with N expressions.
**p2p any-match**

This command allows you to define rule expressions to match all Peer-to-Peer (P2P) packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | p2p any-match operator condition
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

`operator` must be one of the following:

- `=`: Equals

**condition**

Specifies the condition to match.

`condition` must be one of the following:

- `TRUE`: The rule matches any P2P traffic.
- `FALSE`: The rule does not match any P2P traffic.

**Usage Guidelines**

Use this command to define rule expressions to match all P2P packets.
**Examples**

The following command defines a rule expression to match all P2P packets:

```
p2p any-match = TRUE
```
p2p app-identifier

This command allows you to configure application identifiers populated from the plugin and mark the matching flows to a custom-defined protocol (CDP) name.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

[ no ] | p2p app-identifier { quic-sni operator quic_sni_string | tls-cname operator tls_cname_string | tls-sni operator tls_sni_string }

no
If previously configured, deletes the specified configuration from the current ruledef.

quic-sni operator quic_sni_string
Specifies the QUIC Server Name Indication (SNI) field value.
operator specifies how to match and must be one of the following:

• !=: Does not equal
• ==: Equals
• contains: Contains
• ends-with: Ends with
• starts-with: Starts with

quic_sni_string specifies the QUIC server name and must be an alphanumeric string of 1 through 127 characters.

tls-cname operator tls_cname_string
Specifies the common name in the Server Hello message of TLS.
SSL renegotiation is supported for the flows that are marked using "tls-cname" rules. This feature is available only if the plugin is loaded with 20.2 or later builds.

`operator` specifies how to match and must be one of the following:

- `!=`: Does not equal
- `=`: Equals
- `contains`: Contains
- `ends-with`: Ends with
- `starts-with`: Starts with

`tls_cname_string` specifies the common name and must be an alphanumeric string of 1 through 127 characters.

`tls-sni operator tls_sni_string`

Specifies the TLS/SSL Server Name Indication (SNI) field.

`operator` specifies how to match and must be one of the following:

- `!=`: Does not equal
- `=`: Equals
- `contains`: Contains
- `ends-with`: Ends with
- `starts-with`: Starts with

`tls_sni_string` specifies the TLS/SSL server name and must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to configure application identifiers populated from the plugin and mark the matching flows to a custom-defined protocol (CDP) name.

The SNI ruledef supports multi-line-or all-lines or default multi-line-and rule lines. The rule lines configured with "=!" operator will not be optimized.

**Important**

The QUIC SNI Detection feature requires the latest ADC Plugin to be loaded from the adc_y2.x stream along with StarOS changes. The default plugin does not support this feature. Contact your Cisco account representative for more information.

**Examples**

The following command configures the QUIC SNI app-identifier that is set to `fb.com`:

```
p2p app-identifier quic-sni = fb.com
```
**p2p behavioral**

This command allows you to define rule expressions to match behavioral detection type — P2P, Video, VoIP, Behavioral Upload or Behavioral Download.

**Product**
ACS, ADC

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

```
[ no ] p2p behavioral operator behavioral_list
```

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
 Specifies how to match.

`operator` must be one of the following:

- `!=`: Does not equal
- `=:` Equals

**behavioral_list**
Specifies the behavior to match. The behavioral list is the list of supported behavioral detection logic populated from the currently loaded ADC plugin.

`behavioral_list` must be one of the following:

- `download`: Detects unknown flows which are data download using behavioral analysis
- `p2p`: Detects P2P/file sharing protocols using behavioral analysis
- `upload`: Detects unknown flows which are data upload using behavioral analysis
- `video`: Detects video flows using behavioral analysis
• **voip**: Detects VoIP (voice and video) protocols using behavioral analysis

**Usage Guidelines**

Use this command to define rule expressions to detect behavioral protocols. Behavioral P2P and behavioral VoIP are meant for zero day detection of P2P/file sharing protocols and VoIP traffic respectively. Behavioral upload/download is similar to client-server upload/download using HTTP, FTP, SFTP, etc. It must also detect flows of non-standard ports which ECS cannot detect and falls under the client-server model. This feature is disabled by default and meant only for statistical purposes (not for charging purposes). For detection purposes use the `p2p-detection behavioral` command in the ACS Configuration Mode.

**Examples**

The following command specifies to configure behavioral VoIP:

```
p2p behavioral = voip
```
p2p protocol

This command allows you to define rule expressions to match P2P protocol. This command must be used for charging purposes. It must not be used for detection purposes.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | p2p protocol operator protocol |

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be = (equals).

protocol

Specifies the protocol to match.

protocol must be one of the following:

- 8tracks
- actionvoip
- actsync
- adobecconnect
- aimini
- amazoncloud
- amazonmusic
• amazonvideo
• antsp2p
• apple-push
• apple-store
• applejuice
• applemaps
• ares
• armagettron
• avi
• badoo
• baidumovie
• battlefld
• bbm
• beatport
• bitcasa
• bittorrent
• bittorrent-sync
• blackberry-store
• blackberry
• blackdialer
• box
• callofduty
• chikka
• cisco-jabber
• citrix
• clubbox
• clubpenguin
• comodounite
• crackle
• crossfire
• cyberghost
• ddlink
• didi
The **facetime** protocol is available only in 9.0 and in 11.0 and later releases.

The **gamekit** protocol is available only in 9.0 and in 11.0 and later releases.
• go90
• goober
• google-music
• google-push
• google
• googleplay
• googleplus
• gotomeeting
• gtalk
• guildwars
• halflife2
• hamachivpn
• hbogo
• hbonow
• heytell
• hgtv
• hike-messenger
• hls
• hotspotvpn
• hulu
• hyves
• iax
• icall
• icecast
• icloud
• idrive
• igo
• iheartradio
• imesh
• imessage
• imgur
• imo
• implus
• instagram
• iplayer
• iptv
• irc
• isakmp
• iskoot
• itunes
• jabber
• jap
• jumblo
• kakaotalk
• kik-messenger
• kontiki
• kugoo
• kuro
• linkedin
• lync
• magicjack
• manolito
• mapfactor
• mapi
• maplestory
• meebo
• mgcp
• mig33
• mlb
• mojo
• monkey3
• mozy
• msn
• msrp
• mute
• mypeople
• myspace
• nateontalk
• naverline
• navigon
• nbc-sports
• netflix
• netmotion
• newsy
• nimbuzz
• nokia-store
• octoshape
• off
• ogg
• oist
• oovoo
• opendrive
• openft
• openvpn
• operamini
• orb
• oscar
• outlook
• paltalk
• pando
• pandora
• path
• pcanywhere
• periscope
• pinterest
• plingm
• poco
• popo
• pplive
• ppstream
• ps3
• qq
• qqgame
• qqlive
• quake
• quic
• quicktime
• radio-paradise
• rdp
• rdt
• regram
• rfactor
• rhapsody
• rmstream
• rodi
• rynga
• samsung-store
• scydo
• secondlife
• shoutcast
• showtime
• silverlight
• siri
• skinny
• skydrive
• skype
• slacker-radio
• slingbox
• slingtv
• smartvoip
• snapchat
• softether
• sopcast
• soribada
• soulseek
• soundcloud
• spdy
• speedtest
• splashfighter
• spotify
• ssdp
• ssl
• starz
• stealthnet
• steam
• stun
• sudaphone
• svtplay
• tagged
• talkatone
• tango
• teamspeak
• teamviewer
• telegram
• thunder
• tmo-tv
• tor
• truecaller
• truphone
• tumblr
• tunein-radio
• tunnelvoice
• tvants
• tvuplayer
• twitter
• twitch
• ultrabac
• ultrasurf
• univision
• upc-phone
• usenet
• ustream
• usee
• vchat
• veohtv
• vessel
• vevo
• viber
• vine
• voipdiscount
• vopium
• voxer
• vpnx
• vtok
• vtun
• vudu
• warcft3
• waze
• webex
• wechat
• weibo
• whatsapp
• wii
• windows-azure
• windows-store
• winmx
• winny
• wmstream
Usage Guidelines

Use this command to define rule expressions to detect P2P protocols for charging purposes. For detection purposes use the `p2p-detection protocol` command in the ACS Configuration Mode.

Examples

The following command specifies to detect orb protocol for charging purposes:

```
p2p protocol = orb
```
**p2p protocol-group**

This command allows you to define rule expressions to match ADC application/protocol group.

**Product**
ACS, ADC

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | p2p protocol-group operator group_list
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  
  **operator** must be one of the following:
  
  - !=: Does not equal
  - ==: Equals

- **group_list**
  Specifies the ADC application/protocol group to match.
  
  **group_list** must be one of the following:
  
  - **anonymous-access**: Anonymous internet access protocols mainly used for illegal purposes.
  - **business**: Applications/Protocols used for business purposes.
  - **communicator**: Applications/Protocols used mainly for messaging which includes IM, IM based file transfer, VoIP or video chats.
  - **cloud**: Applications/Protocols for cloud service.
  - **e-mail**: Applications/Protocols used for electronic mail.
• **e-news**: Applications/Protocols used for internet news and magazine reading.

• **e-store**: Applications/Protocols used for electronic stores.

• **internet-privacy**: Applications/Protocols used for file transfers.

• **filesharing**: Applications/Protocols used for gaming.

• **gaming**: Standard protocols used in internet.

• **p2p-filesharing**: Applications/Protocols used for creating a virtual network over internet mainly for business purposes.

• **p2p-anon-filesharing**: Peer to Peer application/protocols used for anonymous filesharing.

• **remote-control**: Peer to Peer application/protocols used for filesharing.

• **social-nw-game**: Application/Protocols used for remote management.

• **social-nw-generic**: Application/Protocols used for social networking games.

• **social-nw-videoconf**: Application/Protocols used for social networking.

• **standard**: Application/Protocols used for social network video conference.

• **streaming**: Application/Protocols used for streaming audio and video.

• **untagged**: Default group for protocols not otherwise classified.

**Usage Guidelines**

Use this command to define rule expressions to match ADC protocol group. The list of P2P applications/protocols is populated from the currently loaded P2P plugin.

**Examples**

The following command specifies to detect the **gaming** protocol group:

```
p2p protocol-group = gaming
```
p2p set-app-proto

This command allows you to configure the custom-defined protocol (CDP) name.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**

```
| no | p2p set-app-proto cdp_name_string
```

- **no**
  - If previously configured, deletes the specified configuration from the current ruledef.

- **cdp_name_string**
  - Specifies the name of the custom defined protocol (CDP) for TLS/SSL flows, QUIC flows or any app-identifier matching the ruledef. `cdp_name_string` must be an alphanumeric string of 1 through 19 characters.

**Usage Guidelines**
Use this command to set the CDP name. If the flow/packet matches the rule, the CDP name specified in the ruledef will be taken and the flow will be marked as CDP. If no CDP is configured in the rule, then the flow will be treated as TLS/SSL or QUIC flow.

---

**Important**
The QUIC SNI Detection feature requires the latest ADC Plugin to be loaded from the adc_v2.x stream along with StarOS changes. The default plugin does not support this feature. Contact your Cisco account representative for more information.

**Examples**
The following command configures the custom-defined application protocol name set to facebook:

```
p2p set-app-proto facebook
```
p2p traffic-type

This command allows you to define rule expressions to match the traffic type.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs-ruledef) #

Syntax Description

| no | p2p traffic-type operator traffic_type |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• ==: Equals

traffic_type
Specifies the traffic type to match.
In 11.0 and later releases, traffic_type must be one of the following:

• ads
• audio
• file-transfer
• im
• streaming-video
In 10.0 and earlier releases, the supported traffic_type was voice.

Usage Guidelines
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.

Examples
The following command configures the system to detect video traffic:

`p2p traffic-type = video`
pop3 any-match

This command allows you to define rule expressions to match all Post Office Protocol 3 (POP3) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description

| no | pop3 any-match operator condition

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• ==: Equals

condition

Specifies the condition to match.

condition must be one of the following:

• FALSE
• TRUE

Usage Guidelines

Use this command to define rule expressions to match all POP3 packets.
Examples

The following command defines a rule expression to match all POP3 packets:

```
pop3 any-match = TRUE
```
**pop3 command args**

This command allows you to define rule expressions to match POP3 command arguments.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | pop3 command args | case-sensitive | operator argument |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `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 command argument to match.

*argument* must be an alphanumeric string of 1 through 40 characters, and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match POP3 command argument.

**Examples**

The following command defines a rule expression to match POP3 command argument *test*:

```
pop3 command args = test
```
pop3 command id

This command allows you to define rule expressions to match POP3 command ID.

Product                  ACS

Privilege                Security Administrator, Administrator

Command Modes            Exec > ACS Configuration > Ruledef Configuration
active-charging service  service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description       | no | pop3 command id operator command_id

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• >=: Greater than or equals

command_id
Specifies the command ID to match.
command_id must be an integer from 1 through 12.

Usage Guidelines        Use this command to define rule expressions to match a POP3 command ID.
Examples

The following command defines a rule expression to match POP3 command ID 8:

```plaintext
pop3 command id = 8
```
pop3 command name

This command allows you to define rule expressions to match commands sent within a POP3 packet.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | pop3 command name operator command_name
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.

  - **operator** must be one of the following:
    - !==: Does not equal
    - ==: Equals

- **command_name**
  Specifies the command name to match.

  - **command_name** must be one of the following:
    - apop
    - dele
    - list
    - noop
    - pass
- quit
- retr
- reset
- stat
- top
- uidl
- user

**Usage Guidelines**

Use this command to define rule expressions to match commands sent within POP3 packets.

**Examples**

The following command defines a rule expression to match the `list` command sent in POP3 packets:

`pop3 command name = list`
pop3 mail-size

This command allows you to define rule expressions to match POP3 mail size.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

```
| no | pop3 mail-size { operator mail_size | { range | !range } range_from to range_to }
```

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

- **operator** must be one of the following:
  - !=: Does not equal
  - <=: Lesser 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 start of the range.
  - **range_from** 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 to match.

`mail_size` must be an integer from 1 through 4000000000.

**Usage Guidelines**

Use this command to define rule expressions to match POP3 mail size.

**Examples**

The following command defines a rule expression to match POP3 mail size of 40000:

`pop3 mail-size = 40000`
**pop3 pdu-length**

This command allows you to define rule expressions to match the Protocol Data Unit (PDU) length of POP3 packets equal to the POP3 header plus POP3 payload.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef)#

**Syntax Description**

| no | pop3 pdu-length { operator pdu_length | { range | !range } range_from to range_to } |

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

*operator* must be one of the following:

- !=: Does not equal
- <=: Lesser 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 as 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 to match. `pdu_length` must be an integer from 0 through 65535.

**Usage Guidelines**

Use this command to define rule expressions to match POP3 PDU length (header + payload) in bytes.

**Examples**

The following command defines a rule expression to match PDU length of 1000 bytes:

```plaintext
pop3 pdu-length = 1000
```
pop3 pdu-type

This command allows you to define rule expressions to match POP3 Protocol Data Unit (PDU) type.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
| no | pop3 pdu-type operator pdu_type

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
  • !: Does not equal
  • =: Equals

pdu_type
Specifies the POP3 PDU type to match.
pdu_type must be one of the following:
  • command-packet
  • data-packet
  • relay-packet

Usage Guidelines
Use this command to define rule expressions to match POP3 PDU type.
Examples

The following command defines a rule expression to match POP3 PDU type `relay-packet`:

```
pop3 pdu-type = relay-packet
```
### pop3 previous-state

This command allows you to define rule expressions to match the previous state of POP3 sessions.

#### Product
ACS

#### Privilege
Security Administrator, Administrator

#### Command Modes
```
Exec > ACS Configuration > Ruledef Configuration
```

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:
```
[local] host_name (config-acs-ruledef)#
```

#### Syntax Description
```
| no | pop3 previous-state operator pop3 previous_state
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  **operator** must be one of the following:

  - !==: Does not equal
  - ==: Equals

- **pop3 previous_state**
  
  Specifies the previous state to match.

  **pop3 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 Guidelines**

Use this command to define rule expressions to match a POP3 previous state.

**Examples**

The following command defines a rule expression to match user traffic for a POP3 previous state of *connected*:

```
pop3 previous-state = connected
```
pop3 reply args

This command allows you to define rule expressions to match specified arguments with POP3 reply.

Product  ACS

Privilege  Security Administrator, Administrator

Command Modes  Exec > ACS Configuration > Ruledef Configuration

  active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description  | no | pop3 reply args | case-sensitive | operator argument

  no
If previously configured, deletes the specified rule expression from the current ruledef.

  case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

  operator
Specifies how to match.

  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 reply argument to match.

In 11.0 and earlier releases, *argument* must be an alphanumeric string of 1 through 512 characters, and may contain punctuation characters.

In 12.0 and later releases, *argument* must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match specified arguments within a POP3 reply.

**Examples**

The following command defines a rule expression to match the argument *test* with POP3 replies:

```
pop3 reply args = test
```
**pop3 reply id**

This command allows you to define rule expressions to match POP3 reply ID.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

*active-chargingservice service_name > ruledef ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | pop3 reply id operator reply_id
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- `!=`: Does not equal
- `=`: Equals

**reply_id**

Specifies the POP3 reply ID to match.

*reply_id* must be one of the following:

- `0`: Unknown reply
- `1`: +OK
- `2`: -Error

**Usage Guidelines**

Use this command to define rule expressions to match POP3 reply ID.
**Examples**

The following command defines a rule expression to match POP3 reply ID of 2:

```plaintext
pop3 reply id = 2
```
**pop3 reply status**

This command allows you to define rule expressions to match POP3 reply status.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**  
| no | pop3 reply status operator reply_status |

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  
  - `!=`: Does not equal
  - `=`: Equals

- **reply_status**
  Specifies the reply status to match.
  
  - `+OK`: Reply OK
  - `-ERR`: Reply error

**Usage Guidelines**  
Use this command to define rule expressions to match POP3 reply status.
Examples

The following command defines a rule expression to match POP3 reply status +OK:

```
pop3 reply status = +OK
```
**pop3 session-length**

This command allows you to define rule expressions to match POP3 session-length.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | pop3 session-length { operator session_length | { range | !range } range_from to range_to }
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **session_length**
  Specifies the POP3 session length to match.
  `session_length` must be an integer from 1 through 4000000000.

- **{ 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 as an integer from 1 through 4000000000, but less than or equal to **range to**.

• **range to**: Specifies the end of range of POP3 session as an integer from 1 through 4000000000, but greater than or equal to **range from**.

**Usage Guidelines**

Use this command to define rule expressions to match the total length of POP3 sessions.

**Examples**

The following command defines a rule expression to match a POP3 session length of 40000:

```
pop3 session-length = 40000
```
**pop3 state**

This command allows you to define rule expressions to match the current state of POP3 sessions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | pop3 state operator current_state
```

`no`
If previously configured, deletes the specified rule expression from the current ruledef.

`operator`
Specifies how to match.

`operator` must be one of the following:

- `!=`: Does not equal
- `==`: Equals

`current_state`
Specifies the current state to match.

`current_state` must be one of the following:

- `close`
- `connected`
- `data-transaction`
- `reply-error`
- `reply-ok`
• waiting-for-reply

Usage Guidelines
Use this command to define rule expressions to match the current state of POP3 sessions.

Examples
The following command defines a rule expression to match the POP3 current state close:

```
pop3 state = close
```
**pop3 user-name**

This command allows you to define rule expressions to match POP3 user name.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | pop3 user-name | case-sensitive | operator user_name |
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**case-sensitive**

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

**operator**

Specifies how to match.

*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

Specifies the POP3 user name to match.

user_name must be an alphanumeric string of 1 through 64 characters, and may contain punctuation characters and space.

Usage Guidelines

Use this command to define rule expressions to match POP3 user name.

Examples

The following command defines a rule expression to match POP3 user name test:

pop3 user-name = test
**pptp any-match**

This command allows you to define a rule expression to match all Point-to-Point Tunneling Protocol (PPTP) packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | pptp any-match operator condition
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**operator** must be one of the following:

- `!=`: Does not equal
- `=`: Equals

**condition**

Specifies the condition to match.

**condition** must be one of the following:

- `FALSE`
- `TRUE`

**Usage Guidelines**

Use this command to specify a ruledef to analyze user traffic based on the PPTP any match status.
Examples

The following command creates a PPTP ruledef for analyzing user traffic using a PPTP any match status of \textit{FALSE}:

\texttt{pppt any-match = FALSE}
**pptp ctrl-msg-type**

This command allows you to define rule expressions to match control message type in PPTP packets.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | pptp ctrl-msg-type = message_type
```

- **no**  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **message_type**  
  `message_type` must be one of the following:

  - call-clear-request
  - call-disconnect-notify
  - echo-reply
  - echo-request
  - incoming-call-connected
  - incoming-call-reply
  - incoming-call-request
  - outgoing-call-reply
  - outgoing-call-request
  - set-link-info
  - start-control-connection-reply
  - start-control-connection-request
• stop-control-connection-reply
• stop-control-connection-request
• wan-error-notify

Usage Guidelines
Use this command to define rule expressions to match the control message type in PPTP packets.

Examples
The following command specifies to match \texttt{echo-reply} message type:

\texttt{pptp ctrl-msg-type = echo-reply}
pppoe any-match

This command allows you to define rule expressions to match all PPTP Generic Routing Encapsulation (GRE) packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

| no | pppoe any-match = condition

- no

If previously configured, deletes the specified rule expression from the current ruledef.

- condition

  condition must be one of the following:
  - FALSE
  - TRUE

**Usage Guidelines**

Use this command to define rule expressions to match all PPTP GRE packets.

**Examples**

The following command defines a rule expression to match all PPTP GRE packets:

```
pppoe any-match = TRUE
```
radius any-match

This command allows you to define rule expressions to match all RADIUS packets.

**Product**
- GGSN
- PDSN
- PGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**
```
[ no ] radius any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`
radius any-match

Usage Guidelines
Use this command to define an any-match rule expression to match all RADIUS packets.

Examples
The following command defines an any-match rule expression to match all RADIUS packets:
```
radius any-match = TRUE
```
radius error

This command allows you to define rule expressions to match for errors in RADIUS packets and errors in the RADIUS analyzer.

**Product**
- GGSN
- PDSN
- P-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:
```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | radius error operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`
**Usage Guidelines**

Use this command to define rule expressions to match for errors in RADIUS packets and other errors in RADIUS analyzer.

**Examples**

The following command defines a rule expression to match user traffic based on RADIUS error status of **TRUE**:

```
radius error = TRUE
```
radius state

This command allows you to define rule expressions to match the current state of an RADIUS session.

Product
- GGSN
- PDSN
- P-GW

Privilege
- Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

[ no ] radius state operator radius_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- ==: Equals

radius_state
Specifies the RADIUS state to match.
radius_state must be one of the following:

- auth-req-rcvd: Analyzer received the Access-Request message from the client.
- auth-rsp-fail: Analyzer received the Access-reject message from the server.
- auth-rsp-success: Analyzer received the Access-Accept message from the server as a reply to Access-request.
**Usage Guidelines**  
Use this command to define rule expressions to match the current state of an RADIUS session.

**Examples**  
The following command defines a rule expression to match RADIUS current state `close`:

```
radius state = close
```
rtcp any-match

This command allows you to define rule expressions to match all Real-Time Transport Control Protocol (RTCP) packets.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description

| no | rtcp any-match operator condition |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
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: The rule matches any RTCP traffic.
• FALSE: The rule does not match any RTCP traffic.

Usage Guidelines
Use this command to define rule expressions to match all RTCP packets.
The following command defines a rule expression to match all RTCP packets:

```
rtcp any-match = TRUE
```
rtcp jitter

This command allows you to define rule expressions to match the jitter parameter in RTCP packets.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | rtcp jitter operator jitter |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• >=: Greater than or equals

jitter
Specifies the RTCP inter-arrival jitter value (in milliseconds) to match.
jitter must be an integer from 0 through 4294967295.

Usage Guidelines
Use this command to define rule expressions to match jitter parameter found in the RTCP sender report or receiver report packets.
Examples

The following command matches packets for jitter greater than or equal to 1295 milliseconds:

```
rtcp jitter >= 1295
```
**rtcp parent-proto**

This command allows you to define rule expressions to match the parent protocol of the RTCP flow.

---

**Important**

This command is available only in 8.1 and 9.0 and later releases.

---

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```active-charging service service_name > ruledef ruledef_name```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```rtcp parent-proto [no] operator parent_protocol```  

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.

  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `==`: Equals

- **parent_protocol**
  - Specifies the RTCP parent protocol to match.

  - `parent_protocol` must be one of the following:
    - `rtsp`: Real Time Streaming Protocol
    - `sip`: Session Initiation Protocol
Usage Guidelines

Use this command to define rule expressions to match user traffic based on the parent protocol of the RTCP flow.

Examples

The following command defines a rule expression to match user traffic based on SIP being the parent protocol of the RTCP flow:

```
rtcp parent-proto = sip
```
**rtcp pdu-length**

This command allows you to define rule expressions to match Protocol Data Unit (PDU) length of RTCP packets, (RTCP header + RTCP payload).

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | rtcp pdu-length operator pdu_length
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**operator** must be one of the following:

- `!`: Does not equal
- `<`: Lesser than
- `<=`: Lesser than or equals
- `=`: Equals
- `>=`: Greater than or equals

**pdu_length**

Specifies the RTCP length (in bytes) to match.

In 8.1 and later releases, `pdu_length` must be an integer from 1 through 65535.

In 8.0, `pdu_length` must be an integer from 1 through 2000.

**Usage Guidelines**

Use this command to define rule expressions to match RTCP PDU length (header + payload) in bytes.
Examples

The following command defines a rule expression to match user traffic based on an RTCP PDU length of 10000 bytes:

rtcp pdu-length = 10000
rtcp rtsp-id

This command allows you to define rule expressions to match user traffic based on a Real-time Streaming Protocol (RTSP) ID associated with an RTCP flow.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | rtcp rtsp-id | case-sensitive | operator rtsp_id |

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**case-sensitive**

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

**operator**

Specifies how to match.

* 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
rtsp_id

Specifies the value to match.

rtsp_id must be an alphanumeric string of 1 through 32 characters.

Usage Guidelines

Use this command to define rule expressions to match an RTSP ID associated with an RTCP flow.

Examples

The following command defines a rule expression to match user traffic containing RTSP message ID of test1:

rtcp rtsp-id contains test1
rtcp session-length

This command allows you to define rule expressions to match the total length of RTCP sessions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | rtcp session-length operator session_length |

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**session_length**

Specifies the RTCP total session length (in bytes) to match.

In 8.1 and later releases, `session_length` must be an integer from 1 through 4000000000.

In 8.0, `session_length` must be an integer from 1 through 40000000.

**Usage Guidelines**

Use this command to define rule expressions to match RTCP total session length.
Examples

The following command defines a rule expression to match user traffic for a total RTCP session length of 200000:

\texttt{rtcp session-length = 200000}
rtcp uri

This command allows you to define rule expressions to match URI associated with RTCP flows.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:
```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] rtcp uri [ case-sensitive ] operator uri
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  `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
uri

Specifies the URI to match.

uri must be an alphanumeric string of 1 through 127 characters and may include punctuation characters.

Usage Guidelines

Use this command to define rule expressions to match URI associated with RTCP flow.

Examples

The following command defines a rule expression to match user traffic for RTCP URI `rtsp://www.example.org`:

```
rtcp uri = rtsp://www.example.org
```
rtp any-match

This command allows you to define rule expressions to match all Real-time Transport Protocol (RTP) packets.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**  

```
[ no ] rtp any-match operator condition
```

- **no**  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**  
  Specifies how to match.  
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **condition**  
  Specifies the condition to match.  
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage Guidelines**  
Use this command to define rule expressions to match all RTP packets.
Examples

The following command defines a rule expression to match all RTP packets:

```plaintext
rtp any-match = TRUE
```
**rtp parent-proto**

This command allows you to define rule expressions to match the parent protocol of the RTP flow.

---

**Important**

This command is available only in 8.1 and in 9.0 and later releases.

---

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

| no | rtp parent-proto operator parent_protocol |

no

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- !=: Does not equal
- ==: Equals

**parent_protocol**

Specifies the RTP parent protocol to match.

*parent_protocol* must be one of the following:

- rtsp: Real Time Streaming Protocol
- sip: Session Initiation Protocol
**Usage Guidelines**

Use this command to define rule expressions to match user traffic based on the parent protocol of the RTP flow.

**Examples**

The following command defines a rule expression to match user traffic with parent protocol of the RTP flow being SIP:

```plaintext
rtp parent-proto = sip
```
**rtp pdu-length**

This command allows you to define rule expressions to match PDU length of RTP packets, equal to the RTP header + RTP payload.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | rtp pdu-length operator pdu_length
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `==`: Equals
- `>=`: Greater than or equals

**pdu_length**

Specifies the RTP PDU length (in bytes) to match.

In 8.1 and later releases, *pdu_length* must be an integer from 1 through 65535.

In 8.0, *pdu_length* must be an integer from 1 through 2000.
Usage Guidelines

Use this command to define rule expressions to match PDU length (header + payload) of RTP packets in bytes.

Examples

The following command defines a rule expression to match an RTP PDU length of 1000 bytes:

```
rtppdu-length = 1000
```
**rtp rtsp-id**

This command allows you to define rule expressions to match RTSP ID associated with RTP flows.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | rtp rtsp-id | case-sensitive | operator rtsp_id |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `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
rtsp-id

Specifies the RTSP ID to match.

`rtsp_id` must be an alphanumeric string of 1 through 32 characters.

Usage Guidelines

Use this command to define rule expressions to match RTSP ID associated with RTP flows.

Examples

The following command defines a rule expression to match RTSP message ID of `test1`:

```
rtp rtsp-id contains test1
```
rtp session-length

This command allows you to define rule expressions to match the total length of RTP sessions.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
| no | rtp session-length operator session_length |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• <=: Lesser than or equals
• =: Equals
• >=: Greater than or equals

session_length
Specifies the RTP total session length (in bytes) to match.
In 8.1 and later releases, session_length must be an integer from 1 through 4000000000.
In release 8.0, session_length must be an integer from 1 through 40000000.

Usage Guidelines
Use this command to define rule expressions to match the RTP total session length. The session-length is calculated by adding together the "rtp pdu-length" values of all relevant packets.
Examples

The following command defines a rule expression to match a total RTP session length of 200000:

```
rtp session-length = 200000
```
rtp uri

This command allows you to define rule expressions to match the media URI associated with RTP flows.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | rtp uri | case-sensitive | operator | uri |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `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
uri

Specifies the RTP URI to match.

uri must be an alphanumeric string of 1 through 127 characters. uri allows punctuation characters and excludes the "host" portion.

Usage Guidelines

Use this command to define rule expressions to match media URI associated with RTP flow.

Examples

The following command defines a rule expression to match the RTP URI string rtsp://www.example.org:

```plaintext
rtp uri = rtsp://www.example.org
```
**rtsp any-match**

This command allows you to define rule expressions to match all Real Time Streaming Protocol (RTSP) packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] rtsp any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage Guidelines**

Use this command to define rule expressions to match all RTSP packets.
Examples

The following command defines a rule expression to match all RTSP packets:

```
rtsp any-match = TRUE
```
rtsp content length

This command allows you to define rule expressions to match the content length field in RTSP header.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
[ no ] rtsp content length operator content_length

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
  • !=: Does not equal
  • <=: Lesser than or equals
  • =: Equals
  • >=: Greater than or equals

ccontent_length
Specifies the content length (in bytes) to match.
ccontent_length must be an integer from 0 through 65535.

Usage Guidelines
Use this command to define rule expressions to match "content length" field in RTSP headers.
Examples

The following command defines a rule expression to match content length of 10000 in RTSP headers:

\texttt{rtsp content length = 10000}
rtsp content type

This command allows you to define rule expressions to match the content type field in RTSP headers.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | rtsp content type | case-sensitive | operator content_type |

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.

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 content type to match.

content_type must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

Usage Guidelines

Use this command to define rule expressions to match "content type" field in RTSP headers.

Examples

The following command defines a rule expression to match RTSP content type abc100:

rtsp content type = abc100
**rtsp date**

This command allows you to define rule expressions to match the date field in the RTSP message headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | rtsp date | case-sensitive | operator date |

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**case-sensitive**
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

**operator**
Specifies how to match.

*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 date in RTSP header to match.  
*date* must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

**Usage Guidelines**  
Use this command to define rule expressions to match the "date" field in the RTSP message headers.

**Examples**  
The following command defines a rule expression to match the date *12_04_2006* in RTSP message headers:  
```
rtsp date = 12_04_2006
```
rtsp previous-state

This command allows you to define rule expressions to match the previous state of RTSP sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

[ no ] rtsp previous-state operator rtsp_previous_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- =: Equals

rtsp_previous_state
Specifies the previous state to match.

rtsp_previous_state must be one of the following:

- init
- open
- play
- ready
- record
Usage Guidelines

Use this command to define rule expressions to match the previous state of RTSP sessions.

Examples

The following command defines a rule expression to match RTSP previous state ready:

\texttt{rtsp previous-state = ready}
rtsp reply code

This command allows you to define rule expressions to match the return code in RTSP responses.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
[ no ] rtsp reply code operator reply_code

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• >=: Greater than or equals

reply_code
Specifies the RTSP reply code to match.
reply_code must be an integer from 100 through 599.

Usage Guidelines
Use this command to define rule expressions to match the return code in RTSP response.
Examples

The following command defines a rule expression to match RTSP return code 302:

```
rtsp reply code = 302
```
**rtsp request method**

This command allows you to define rule expressions to match the method in RTSP responses.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] rtsp request method operator request_method
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `=`: Equals

- **request_method**
  - Specifies the RTSP request method to match.
  - `request_method` must be one of the following requests:
    - `announce`
    - `describe`
    - `get-parameter`
    - `options`
    - `pause`
• play
• record
• redirect
• set-parameter
• setup
• teardown

Usage Guidelines
Use this command to define rule expressions to match the method in RTSP responses.

Examples
The following command defines a rule expression to match RTSP request method announce:

```plaintext
rtsp request method = announce
```
rtsp request packet

This command allows you to define rule expressions to match all RTSP request messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | rtsp request packet | operator | condition |

no
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

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: Is request
- FALSE: Is response

**Usage Guidelines**
Use this command to define rule expressions to match all RTSP request messages.
Examples

The following command defines a rule expression to match all RTSP request messages:

```
rtsp request packet = TRUE
```
rtsp rtp-seq

This command allows you to define rule expressions to match the "seq" field in the RTP-Info header of RTSP responses.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | rtsp rtp-seq operator sequence_number |
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `=`: Equals
- `>=`: Greater than or equals

**sequence_number**

Specifies the sequence number in the RTSP RTP-Info field to match.

*sequence_number* must be an alphanumeric string of 0 through 65535 characters in Normal Play Time (NPT) time format.
Usage Guidelines

Use this command to define rule expressions to match user traffic matching the "seq" field in the RTP-Info header of RTSP response for a PLAY request.

Examples

The following command defines a rule expression to match user traffic based on RTP-seq number npt-12:34:59:

```
rtsp rtp-seq = npt-12:34:59
```
rtsp rtp-time

This command allows you to define rule expressions to match the "time" field in RTP-Info header of RTSP responses.

Product ACS

Privilege Security Administrator, Administrator

Command Modes

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | rtsp rtp-time operator time |

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

time

Specifies the time to match.

time must be an alphanumeric string of 1 through 2147483647 characters in Normal Play Time (NPT) time format.
Usage Guidelines

Use this command to define rule expressions to match the "time" field in the RTP-Info header of RTSP response for a PLAY request.

Examples

The following command defines a rule expression to match RTP timestamp of 20120123T153600Z:

rtsp rtp-time = 20120123T153600Z
rtsp rtp-uri

This command allows you to define rule expressions to match the URI field in the RTP-Info header of RTSP responses.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

| no | rtsp rtp-uri | case-sensitive | operator uri |

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  - Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  - Specifies how to match.
  - `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
uri

Specifies the value to match with the URI in RTP-Info header of the RTSP message.

uri must be an alphanumeric string of 1 through 127 characters. uri allows punctuation characters and excludes the "host" portion.

Usage Guidelines

Use this command to define rule expressions to match the URI field in the RTP-Info header of the RTSP response for a PLAY request.

Examples

The following command defines a rule expression to match user traffic based on RTP-URI string rtsp://www.foo.com in the RTP-info header of RTSP packet:

rtsp rtp-uri = rtsp://www.foo.com
rtsp session-id

This command allows you to define rule expressions to match the session ID in RTSP messages.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] rtsp session-id [ case-sensitive ] operator session_id
```

- **no**  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**  
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**  
  Specifies how to match.

  **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**

Specifies the session ID to match.

*session_id* must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to define rule expressions to match the session ID in RTSP messages.

**Examples**

The following command defines a rule expression to match the RTSP session ID 0123abc100:
```
rtsp session-id = 0123abc100
```
rtsp session-length

This command allows you to define rule expressions to match the total length of RTSP sessions.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | rtsp session-length operator session_length |

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- =: Equals
- >=: Greater than or equals

session_length

Specifies the RTSP session length (in bytes) to match.

session_length must be an integer from 1 through 4000000.

Usage Guidelines

Use this command to define rule expressions to match the total length of RTSP sessions. That is, the sum of the "rtsp pdu-length" values of all relevant packets.
### Examples

The following command defines a rule expression to match RTSP session length of 3000000 bytes:

```
rtsp session-length = 3000000
```
rtsp state

This command allows you to define rule expressions to match the current state of RTSP sessions.

Product  ACS

Privilege  Security Administrator, Administrator

Command Modes  Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acrs-ruledef)#

Syntax Description  | no | rtsp state operator current_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- ==: Equals

current_state
Specifies the current state to match.

current_state must be one of the following:

- end
- init
- open
- play
- ready
• record

**Usage Guidelines**  
Use this command to define rule expressions to match the current state of RTSP sessions.

**Examples**  
The following command defines a rule expression to match RTSP current state `init`:

```
rtsp state = init
```
**rtsp uri**

This command allows you to define rule expressions to match URI in RTSP request message.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```plaintext
[ no ] rtsp uri | case-sensitive | operator uri
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  - Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  - Specifies how to match.
  - `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
    - `regex`: Regular expression
- **starts-with**: Starts with

**uri**

Specifies the URI to match.

*uri* must be an alphanumeric string of 1 through 127 characters. *uri* allows punctuation characters and excludes the "host" portion.

**Usage Guidelines**

Use this command to define rule expressions to match URI in RTSP request.

The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the Enhanced Charging Service Administration Guide.

**Table 10: Special Characters Supported in Regex Rule Expressions**

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>?</td>
<td>Match zero or one character</td>
</tr>
<tr>
<td>?</td>
<td>Match the question mark (&lt;ctrl-v&gt;?) character</td>
</tr>
<tr>
<td>+</td>
<td>Match the plus character</td>
</tr>
<tr>
<td>\*</td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td>\a</td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td>\b</td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td>\f</td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
<tr>
<td>\n</td>
<td>Match the New line (ASCII 10) character</td>
</tr>
</tbody>
</table>
### Regex Character

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\r</td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td>\t</td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td>\v</td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td>\0</td>
<td>Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td>\</td>
<td>Match the backslash character</td>
</tr>
<tr>
<td>Bracketed range [0-9]</td>
<td>Match any single character from the range</td>
</tr>
<tr>
<td>^</td>
<td>Do not match any in the range. All other characters represent themselves.</td>
</tr>
<tr>
<td>\x##</td>
<td>Any ASCII character as specified in two-digit hex notation. For example, \x5A yields a &quot;Z&quot;.</td>
</tr>
<tr>
<td></td>
<td>Specify OR regular expression operator</td>
</tr>
</tbody>
</table>

**Important** When using the regex operator "\|" in regex expressions, always wrap the string in double quotes. For example, if you want to match the string "pqr" OR "xyz", you must configure it as:

```plaintext
http host regex "pqr|xyz".
```

### Examples

The following command defines a rule expression to match user traffic based on RTSP URI

```
rtsp://www.example.com:554/twister/audiotrack:
```

The following command defines a regex rule expression to match either of the following or similar values in the RTSP URI string: rtsp://pvs29p.cvf.fr:554/t1/live/Oui17, rtsp://pvs00p.cvf.fr:554/t1/live/Nrj12, rtsp://pvs90p.cvf.fr:554/t1/live/France24_fr.

```
rtsp uri regex "rtsp://(0-9)(0-9)p.cvf.fr:554/t1/live/(Gulli|Tf1|Tmc|Nrj12|Star|France24_fr|Oui17)*"
```
rtsp uri sub-part

This command allows you to define rule expressions to match user traffic by parsing sub-parts of the URI in an RTSP request message.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef) #

Syntax Description

| no | rtsp uri sub-part { { absolute-path | host | query } | case-sensitive | operator string | port { port_operator port_value | { range | !range } range_from to range_to } }

no
If previously configured, deletes the specified rule expression from the current ruledef.

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
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
string
Specifies the absolute path/host name or query string to match with the URI in RTSP header.
A string must be an alphanumeric string of 1 through 127 characters. string allows punctuation characters and excludes the "host" portion.

port
Specifies the port related matching for RTSP URI in an RTSP request message.

port_operator
Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equal
- =: Equals
- >=: Greater than or equal

port_value
Specifies the RTSP port number to match with port rule in the RTSP flow as 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 as 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 as an integer from 0 through 65535, but more than or equal to range_from.
Usage Guidelines

Use this command to define rule expressions to match URI sub parts like host, absolute path, port, and query in RTSP request messages.

Examples

The following command defines a URI sub part rule expression to analyze user traffic based on an RTSP URI port number between 1023 and 1068:

```
rtsp uri sub-part port range 1023 to 1068
```
**rtsp user-agent**

This command allows you to define rule expressions to match the user-agent field in RTSP headers.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

`[no] rtsp user-agent [case-sensitive] [operator user_agent]`

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  `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 to match.

user_agent must be an alphanumeric string of 1 through 127 characters.

### Usage Guidelines

Use this command to define rule expressions to match the "user-agent" field in RTSP header.

### Examples

The following command defines a rule expression to match test in "user-agent" field of RTSP header:

```
rtsp user-agent = test
```
rtsp-stream any-match

This command allows you to define rule expressions to match all user traffic of type RTSP, RTCP, and RTP to achieve an unified charging for RTSP correlated flows.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
[ no ] rtsp-stream any-match operator condition

no
If previously configured, deletes the rtsp-stream any match 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 to match.
condition must be one of the following:
  • FALSE
  • TRUE

Usage Guidelines
Use this command to specify a rule definition to analyze all RTSP, RTCP, and RTP traffic.
Example

The following command defines a rule expression to match all RTSP, RTCP, and RTP user traffic:

```
rtsp-stream any-match = TRUE
```
rtsp-stream first-setup-url

This command allows you to define rule expressions to match user traffic of type RTSP, RTCP, and RTP on the first setup URL of the parent RTSP flow to achieve an unified charging for RTSP correlated flows.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

```
[no] rtsp-stream first-setup-url | case-sensitive | operator url
```

- **no**
  If previously configured, deletes the rtsp-stream any match rule definition.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions 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
  - `regex`: Regular expression
**starts-with**: Starts with

**url**
Specifies the URL to match.

* url must be an alphanumeric string of 1 through 127 characters.

### Usage Guidelines

Use this command to specify a rule definition to analyze RTSP, RTCP, and RTP traffic based on the first setup URL of the parent RTSP flow.

The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the *Enhanced Charging Service Administration Guide*.

**Table 11: Special Characters Supported in Regex Rule Expressions**

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>?</td>
<td>Match zero or one character</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>The CLI does not support configuring &quot;?&quot; directly, you must instead use &quot;\077&quot;.</td>
</tr>
<tr>
<td></td>
<td>For example, if you want to match the string &quot;xyz&lt;any one character&gt;pqr&quot;, you must configure it as:</td>
</tr>
<tr>
<td><strong>http host regex</strong></td>
<td>&quot;xyz\077pqr&quot;</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>In another example, if you want to exactly match the string &quot;url?resource=abc&quot;, you must configure it as:</td>
</tr>
<tr>
<td><strong>http uri regex</strong></td>
<td>&quot;url\077resource=abc&quot;</td>
</tr>
<tr>
<td>\</td>
<td>Escaped character</td>
</tr>
<tr>
<td>?</td>
<td>Match the question mark (&lt;ctrl-v&gt;?) character</td>
</tr>
<tr>
<td>+</td>
<td>Match the plus character</td>
</tr>
<tr>
<td>*</td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td>\a</td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td>\b</td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td>\f</td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
<tr>
<td>\n</td>
<td>Match the New line (ASCII 10) character</td>
</tr>
</tbody>
</table>
### Regex Character

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>\r</code> Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td><code>\t</code> Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td><code>\v</code> Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td><code>\0</code> Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td><code>\</code> Match the backslash character</td>
</tr>
<tr>
<td>Bracketed range [0-9] Match any single character from the range</td>
</tr>
<tr>
<td>A leading ^ in a range Do not match any in the range. All other characters represent themselves.</td>
</tr>
<tr>
<td><code>.\</code> Any ASCII character as specified in two-digit hex notation. For example, <code>\x5A</code> yields a &quot;Z&quot;.</td>
</tr>
<tr>
<td>`</td>
</tr>
</tbody>
</table>

#### Important

When using the regex operator "|" in regex expressions, always wrap the string in double quotes.

For example, if you want to match the string "pqr" OR "xyz", you must configure it as:

```
http host regex "pqr|xyz".
```

### Example

The following command defines a rule expression to match all RTSP, RTCP, and RTP traffic when the parent RTSP's first setup URL contains `cisco.com`:

```
rtsp-stream first-setup-url contains cisco.com
```

The following command defines a rule expression to match all RTSP, RTCP, and RTP traffic when the parent RTSP's first setup URL matches the given regular expression:

```
rtsp://tvs100.google.fr/t1/M6
```

```
rtsp-stream first-setup-url regex rtsp://tvs(a|l|b)[0-9][0-9].google.(fr|:554)/t1/(M6|W9_)*
```
rule-application

This command allows you to specify the purpose of a ruledef, such as for charging, post-processing, routing, and so on.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs-ruledef) #

**Syntax Description**

```
rule-application { charging | post-processing | routing | tpo }
no rule-application
```

- **charging**
  Specifies that the current ruledef is for charging purposes.
  Up to 2,048 rule definitions can be defined for the charging application in an Active Charging Service.
  Default: Enabled

- **post-processing**
  The `post-processing` keyword is available only in 8.3 and later releases.
  Specifies that the current ruledef is for post-processing purposes. This enables processing of packets even if the rule matching for them has been disabled.

- **routing**
  Specifies that the current ruledef is for routing purposes. Up to 256 rule definitions can be defined for routing in an Active Charging Service. Default: Disabled
The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

**Usage Guidelines**

Use this command to specify the rule application for 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.

**Examples**

The following command configures the rule application "charging" to the current rule definition:

```
rule-application charging
```
**sdp any-match**

This command allows you to define rule expressions to match all packets that contain Session Description Protocol (SDP) descriptions.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
[local] <host_name> (config-acs-ruledef) #
```

**Syntax Description**

```
| no | sdp any-match operator condition |
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!:` Does not equal
    - `=`: Equals

- **condition**
  - Specifies the condition to match.
  - `condition` must be one of the following:
    - `FALSE`
    - `TRUE`

**Usage Guidelines**

Use this command to define rule expressions to match all packets containing SDP descriptions.
Examples

The following command defines a rule expression to match all packets containing SDP descriptions:

```
sdp any-match = TRUE
```
sdp connection-ip-address

This command allows you to define rule expressions to match the IP address in the connection field of SDP descriptions.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description
| no | sdp connection-ip-address operator ipv4_address |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- ==: Equals

ipv4_address
Specifies the IP address to match.
ipv4_address must be in IPv4 dotted-decimal notation.

Usage Guidelines
Use this command to define rule expressions to match IP address in the connection field of SDP descriptions.
Examples

The following command defines a rule expression to match the IP address 10.1.1.1 in the connection field of SDP descriptions:

sdp connection-ip-address = 10.1.1.1
sdp media-audio-port

This command allows you to define rule expressions to match media audio ports specified in the media sections of SDP descriptions.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | sdp media-audio-port operator port |

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`operator`

Specifies how to match.

`operator` must be one of the following:

- !: Does not equal
- =: Equals

`port`

Specifies the port number to match.

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

**Usage Guidelines**

Use this command to define rule expressions to match media audio ports specified in the media sections of SDP descriptions.
**Examples**

The following command defines a rule expression to match media audio port 100 in the media sections of SDP descriptions:

```
sdp media-audio-port = 100
```
sdp media-video-port

This command allows you to define rule expressions to match media video ports specified in the media sections of SDP descriptions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

```
no
```

If previously configured, deletes the specified rule expression from the current ruledef.

```
operator port
```

Specifies how to match.

- `!=`: Does not equal
- `=:` Equals

```
port
```

Specifies the port number to match.

*port* must be an integer from 0 through 65535.

**Usage Guidelines**
Use this command to define rule expressions to match media video ports specified in the media sections of SDP descriptions.
Examples

The following command defines a rule expression to match media video port 100 in the media sections of SDP descriptions:

```
sdp media-video-port = 100
```
sdp uplink

This command allows you to define rule expressions to match SDP descriptions in the uplink (subscriber to network) direction.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef)#

Syntax Description

| no | sdp uplink operator condition

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- ==: Equals

condition

Specifies the condition to match.

condition must be one of the following:

- FALSE: Is not uplink
- TRUE: Is uplink

Usage Guidelines

Use this command to define rule expressions to match SDP descriptions in uplink direction.
Examples

The following command defines a rule expression to match all SDP descriptions in the uplink direction:

```
sdp uplink = TRUE
```
secure-http any-match

This command allows you to define rule expressions to match all Secure HTTP (HTTPS) packets.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | secure-http any-match operator condition

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• ==: Equals

condition

Specifies the condition to match.

condition must be one of the following:

• FALSE
• TRUE

Usage Guidelines Use this command to define rule expressions to match all Secure HTTP packets.
Examples

The following command defines a rule expression to match all HTTPS packets:

```
secure-http any-match = TRUE
```
secure-http uplink

This command allows you to define rule expressions to match uplink (subscriber to network) HTTPS packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**

```
| no | secure-http uplink operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.

  `operator` must be one of the following:

  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  Specifies the condition to match.

  `condition` must be one of the following:

  - `FALSE`: Is not uplink
  - `TRUE`: Is uplink

**Usage Guidelines**
Use this command to define rule expressions to match uplink HTTPS packets.
Examples

The following command defines a rule expression to match all uplink HTTPS packets:

```
secure-http uplink = TRUE
```
**sip any-match**

This command allows you to define rule expressions to match all Session Initiation Protocol (SIP) packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | sip any-match operator condition |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage Guidelines**

Use this command to define rule expressions to match all SIP packets.
Examples

The following command defines a rule expression to match all SIP packets:

```
sip any-match = TRUE
```
**sip call-id**

This command allows you to define rule expressions to match the Call ID in SIP messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```plaintext
| no | sip call-id | case-sensitive | operator call_id |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  ```plaintext
  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**

Specifies the call ID to match.

*call-id* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match the call ID in SIP messages.

**Examples**

The following command defines a rule expression to match the call ID *test* in SIP messages:

```
sip call-id = test
```
sip content length

This command allows you to define rule expressions to match the content-length field in SIP headers.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

```plaintext
| no | sip content length operator content_length
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

* operator must be one of the following:
  - !=: Does not equal
  - <=: Lesser than or equals
  - ==: Equals
  - >=: Greater than or equals

**content_length**

Specifies the SIP content length to match.

* content_length must be an integer from 0 through 65535.

**Usage Guidelines**

Use this command to define rule expressions to match the content-length field in SIP headers.
**Examples**

The following command defines a rule expression to match the content length 10000 in SIP headers:

```
sip content length = 10000
```
sip content type

This command allows you to define rule expressions to match the content type field in SIP headers.

**Product**  ACS

**Privilege**  Security Administrator, Administrator

**Command Modes**  Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**

```
| no | sip content type | case-sensitive | operator content_type |
```

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

**operator**

Specifies how to match.

*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 content type to match.

*content_type* must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to define rule expressions to match the content type field in SIP headers.

**Examples**

The following command defines a rule expression to match content type *download_string* in SIP headers:

```
sip content type = download_string
```
**sip from**

This command allows you to define rule expressions to match the from field in SIP messages.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | sip from | case-sensitive | operator string
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  **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
**Usage Guidelines**

Use this command to define rule expressions to match the "from" field in SIP messages.

**Examples**

The following command defines a rule expression to match `test1` in the "from" field in SIP messages:

```
sip from contains test1
```
sip previous-state

This command allows you to define rule expressions to match previous state of SIP sessions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**

`Exec > ACS Configuration > Ruledef Configuration`

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

`[local]host_name(config-acs-ruledef)#`

**Syntax Description**

`| no | sip previous-state operator sip_previous_state`

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **sip_previous_state**
  Specifies the previous state to match.
  `sip_previous_state` must be one of the following:
  - `init`
  - `provisional-response`
  - `request-sent`
  - `response-fail`
  - `response-ok`
**Usage Guidelines**

Use this command to define rule expressions to match a previous state of SIP sessions.

**Examples**

The following command defines a rule expression to match user traffic based on the SIP previous state of `request-sent`:

```
sip previous-state = request-sent
```
**sip reply code**

This command allows you to define rule expressions to match the reply code in SIP responses.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```text
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**

```text
| no | sip reply code operator reply_code
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**operator** must be one of the following:

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `=`: Equals
- `>=`: Greater than or equals

**reply_code**

Specifies the SIP reply code to match.

**reply_code** must be an integer from 100 through 699.

**Usage Guidelines**

Use this command to define rule expressions to match the reply code in SIP responses.
Examples

The following command defines a rule expression to match 180 in the reply code in SIP responses:

```
sip reply code = 180
```
**sip request method**

This command allows you to define rule expressions to match the method in SIP requests.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | sip request method operator method
```

no
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

`operator` must be one of the following:

- `!`: Does not equal
- `=`: Equals

**method**

Specifies the SIP method to match.

`method` must be one of the following:

- `ack`
- `bye`
- `cancel`
- `info`
- `invite`
- message
- notify
- options
- prack
- publish
- refer
- register
- subscribe
- update

**Usage Guidelines**
Use this command to define rule expressions to match the method in SIP requests.

**Examples**
The following command defines a rule expression to match the method **bye** in SIP request messages:

```plaintext
sip request method = bye
```
sip request packet

This command allows you to define rule expressions to match all SIP request packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef)#
```

**Syntax Description**

```
| no | sip request packet operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  The `operator` must be one of the following:
  - `=`: Equals
  - `!=`: Does not equal

- **condition**
  Specifies the condition to match.
  The `condition` must be one of the following:
  - `FALSE`: Is a response
  - `TRUE`: Is a request

**Usage Guidelines**
Use this command to define rule expressions to match all SIP request packets.
**Examples**

The following command defines a rule expression to match all SIP request packets:

```
sip request packet = TRUE
```
**sip state**

This command allows you to define rule expressions to match current state of the SIP session.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration  
**active-charging service service_name > ruledef ruledef_name**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**  

```  
[no] sip state operator current_state
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

- `!=`: Does not equal
- `=`: Equals

**current_state**

Specifies the current state to match.

- `ack-received`
- `provisional-response`
- `request-sent`
- `response-fail`
- `response-ok`
Usage Guidelines

Use this command to define rule expressions to match the current SIP session.

Examples

The following command defines a rule expression to match user traffic based on SIP current state `request-sent`:

```
sip state = request-sent
```
**sip to**

This command allows you to define rule expressions to match the "to" field in SIP messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | sip to | case-sensitive | operator to_address |

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.

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_address

Specifies the "to" address/name to match.
to_address must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage Guidelines

Use this command to define rule expressions to match the "to" field in SIP messages.

Examples

The following command defines a rule expression to match test1 in the "to" field of SIP messages:

sip to contains test1
This command allows you to define rule expressions to match the URI in SIP messages.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

Command Syntax
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | sip uri | sub-part { headers | host | parameters | port | userinfo } | | case-sensitive | operator uri |

no
If previously configured, deletes the specified rule expression from the current ruledef.

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
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:

- !=: Does not equal
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
- `=`: Equals
- `>`: Is greater than

**uri**

Specifies the SIP URI to match.

`uri` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

The string for sub-part keyword `port` must be an integer from 0 through 65535.

**Usage Guidelines**

Use this command to define rule expressions to match the URI in SIP messages.

**Examples**

The following command defines a rule expression to match the URI string `sip:10.1.1.1:5060` in SIP messages:

```
sip uri = sip:10.1.1.1:5060
```

The following command defines a rule expression to match the URI string `sip:nnnn@host:5060;user=phone` in SIP messages:

```
sip uri = sip:nnnn@host:5060;user=phone
```
smtp any-match

This command allows you to define rule expressions to match all Simple Mail Transfer Protocol (SMTP) packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

`active-chargingservice service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

`[local] host_name(config-acs-ruledef)#`

**Syntax Description**

`[no] smtp any-match operator condition`

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage Guidelines**
Use this command to define rule expressions to match all SMTP packets.
Examples

The following command defines a rule expression to match all SMTP packets:

`smtp any-match = TRUE`
smtp command arguments

This command allows you to define rule expressions to match SMTP command arguments.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | smtp command arguments | case-sensitive | operator argument |

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
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 command argument to match.

*argument* must be an alphanumeric string of 1 through 63 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match SMTP command arguments.

**Examples**

The following command defines a rule expression to match SMTP command argument *test*:

```
smtp command arguments = test
```
smtp command id

This command allows you to define rule expressions to match SMTP command IDs.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | smtp command id operator command_id |

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• >=: Greater than or equals

command_id

Specifies the command argument to match.

command_id must be an integer from 0 through 10.

Usage Guidelines

Use this command to define rule expressions to match SMTP command IDs.
Examples

The following command defines a rule expression to match SMTP command ID 8:

\texttt{smtp command id = 8}
smtp command name

This command allows you to define rule expressions to match commands sent in SMTP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**
```
| no | smtp command name operator command_name
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  ```plaintext
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals
  ```

- **command_name**
  Specifies the command name to match.
  ```plaintext
  command_name must be one of the following:
  - bdat
  - data
  - ehlo
  - expn
  - helo
  ```
Usage Guidelines
Use this command to define rule expressions to match commands sent in SMTP packets.

Examples
The following command defines a rule expression to match data command in SMTP packets:
```
smtplib command name = data
```
smtp mail-size

This command allows you to define rule expressions to match the size of mail sent by a SMTP client.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
no | smtp mail-size { operator mail_size | { { range | !range } range_from to range_to } }
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  - **operator** must be one of the following:
    - `!=`: Does not equal
    - `<=`: Lesser than or equals
    - `==`: Equal
    - `>=`: Greater than or equals

- **mail_size**
  
  Specifies the mail size (in bytes) to match.

  - **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 as 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 Guidelines
Use this command to define rule expressions to match the size of mail sent by an SMTP client.

Examples
The following command defines a rule expression to match mail size of 40000 bytes:

smtp mail-size = 40000
smtp pdu-length

This command allows you to define rule expressions to match the Protocol Data Unit (PDU) length of SMTP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description
| no | smtp pdu-length { operator pdu_length | { range | !range } range_from to range_to } |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- =: Equals
- >=: Greater than or equals

pdu_length
Specifies the SMTP PDU length (in bytes) to match.
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 as 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 Guidelines**

Use this command to define rule expressions to match PDU length of SMTP packets, that is headers + payload.

**Examples**

The following command defines a rule expression to match a PDU length of 1600 bytes:

```
smtppdu-length = 1600
```
smtp previous-state

This command allows you to define rule expressions to match previous state of SMTP command sessions.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description

| no | smtp previous-state operator smtp_previous_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• =: Equals

smtp_previous_state
Specifies the previous state to match.
smtp_previous_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 Guidelines

Use this command to define rule expressions to match a previous state of SMTP command sessions.

Examples

The following command defines a rule expression to match user traffic based on SMTP previous state close:

```
smtplib previous-state = close
```
smtp recipient

This command allows you to define rule expressions to match the recipient e-mail ID in the current SMTP transaction.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
no | smtp recipient | case-sensitive | operator argument
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

`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 response argument to match.

*argument* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match the recipient e-mail ID in the current SMTP transaction.

**Examples**

The following command defines a rule expression to match recipient e-mail ID containing *test* in the current SMTP transaction:

```plaintext
smtp recipient contains test
```
smtp reply arguments

This command allows you to define rule expressions to match the arguments within SMTP responses.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

`[local]<host_name>(config-acs-ruledef)#`

**Syntax Description**

`| no | smtp reply arguments | case-sensitive | operator argument`

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  
  Specifies how to match.

  `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 reply argument to match.

*argument* must be an alphanumeric string of 1 through 63 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match the arguments with SMTP response.

**Examples**

The following command defines a rule expression to match reply argument *forward-path* in SMTP response:

`smtp reply arguments = forward-path`
smtp reply id

This command allows you to define rule expressions to match reply ID assigned to SMTP responses.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

```
[no] smtp reply id operator reply_id
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  
  **operator** must be one of the following:
  
  - `!=`: Does not equal
  - `=`: Equals

- **reply_id**
  Specifies the reply ID to match.
  
  **reply_id** must be one of the following:
  
  - `0`: +NO reply
  - `1`: +OK reply
  - `2`: -ERR reply

**Usage Guidelines**
Use this command to define rule expressions to reply ID assigned to SMTP response.
Examples

The following command defines a rule expression to match reply ID 2 assigned to SMTP response:

\texttt{smtp reply id = 2}
smtp reply status

This command allows you to define rule expressions to match the reply status in SMTP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
| no | smtp reply status operator reply_status

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

reply_status
Specifies the SMTP reply status to match.
reply_status must be one of the following:
• +OK: Response OK
• -ERR: Response error

Usage Guidelines
Use this command to define rule expressions to match reply status in SMTP packets.
Examples

The following command defines a rule expression to match reply status +OK in SMTP packets:

```
smtp reply status = +OK
```
smtp sender

This command allows you to define rule expressions to match sender e-mail ID in the current SMTP transaction.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]\host_name(config-acs-ruledef)#

Syntax Description

| no | smtp sender | case-sensitive | operator sender |

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.

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 sender value to match.

sender must be an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to define rule expressions to match sender e-mail ID in the current SMTP transaction.

Examples

The following command defines a rule expression to match sender e-mail ID containing test in the current SMTP transaction:

```
smtplib sender contains test
```
smtp session-length

This command allows you to define rule expressions to match total length of SMTP sessions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax Description**

```plaintext
[ no ] smtp session-length { operator session_length | { range | !range } range_from to range_to }
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!`: Does not equal
    - `<=`: Lesser than or equals
    - `=`: Equals
    - `>=`: Greater than or equals

- **session_length**
  - Specifies the session length to match.
  - `session_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 as 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 Guidelines**

Use this command to define rule expressions to match total length of SMTP session.

**Examples**

The following command defines a rule expression to match SMTP session length of 4000000:

```
smtplib session-length = 4000000
```
smtp state

This command allows you to define rule expressions to match current state of a SMTP command session.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
| no | smtp state operator current_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
  • !=: Does not equal
  • =: Equals

current_state
Specifies the current state to match.
current_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 Guidelines

Use this command to define rule expressions to match current state of SMTP command session.

Examples

The following command defines a rule expression to match current state as close of SMTP command session:

```
smtplib state = close
```
tcp analyzed out-of-order

This command allows you to define rule expressions to determine whether the received TCP packet was received before all of the earlier sequenced packets have been received. This functionality is for whether the packet was analyzed or discarded because the earlier sequenced packet(s) was (were) not received before a timeout expired.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs-ruledef) #

Syntax Description
| no | tcp analyzed out-of-order operator condition |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• ==: Equals

condition
Specifies the condition to match.

ccondition must be one of the following:

• FALSE: Not analyzed
• TRUE: Analyzed
Usage Guidelines

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), it and subsequent packets are buffered at ACSMgr/SessMgr as TCP out-of-order packets and ACSMgr/SessMgr waits for missing packet(s) until the time-out duration expires. If the packet(s) with the missing sequence number(s) arrives within the time-out duration, all buffered packets with the 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 the TCP/IP layer only.

If this command is enabled the TCP out-of-order packets are marked and sent to TCP analyzer as analyzed for charging action, otherwise they are discarded.

Examples

The following command sets to analyze TCP out-of-order packets:

tcp analyzed out-of-order = TRUE
tcp any-match

This command allows you to define rule expressions to match all TCP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```text
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**

```
| no | tcp any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - operator must be one of the following:
    - !=: Does not equal
    - ==: Equals

- **condition**
  Specifies the condition to match.
  - condition must be one of the following:
    - FALSE: Not analyzed
    - TRUE: Analyzed

**Usage Guidelines**
Use this command to define rule expressions to match all TCP packets.
Examples

The following command defines a rule expression to match all TCP packets:
```
tcp any-match = TRUE
```
**tcp client-port**

This command allows you to define rule expressions to match client port number in TCP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef)#
```

**Syntax Description**

```plaintext
[ no | tcp client-port { operator port_number | !range range } { start_range to end_range | port-map port_map_name } ]
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `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_name_

Specifies the port map for the port range. _port_map_name_ must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to define rule expressions to match a client port number in TCP headers.

**Examples**

The following command defines a rule expression to analyze user traffic matching TCP client port 5000:

tcp client-port = 5000
**tcp connection-initiator**

This command allows you to define rule expressions to match the TCP connection initiator.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

*active-charging service service_name > ruledef ruledef_name*

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | tcp connection-initiator operator subscriber |

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- !==: Does not equal
- ==: Equals

**subscriber**

Specifies that the connection is being initiated by the subscriber.

**Usage Guidelines**

Use this command to define rule expressions to match the TCP connection initiator, and to allow the operator to differentiate when the connection initiated by subscriber or the subscriber is acting as a Transaction Control Server (TCS) server.

**Examples**

The following command defines a rule expression to match user traffic based on TCP connection initiator subscriber:

```
tcp connection-initiator = subscriber
```
tcp downlink

This command allows you to define rule expressions to match downlink (network to subscriber) TCP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | tcp downlink operator condition |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• ==: Equals

condition
Specifies the condition to match.

condition must be one of the following:

• FALSE
• TRUE

Usage Guidelines
Use this command to define rule expressions to match downlink (to subscriber) TCP packets.
The following command defines a rule expression to match downlink TCP packets:

```
tcp downlink = TRUE
```
**tcp dst-port**

This command allows you to define rule expressions to match destination port number in TCP headers.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

**Command Line Interface Reference, Commands A - B, StarOS Release 20**

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

```
[ no ] tcp dst-port { operator port_number | !range | range } { start_range to end_range | port-map port_map_name }
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**operator** must be one of the following:

- !=: Does not equal
- <=: Lesser 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_name**

Specifies the port map for the port range. **port_map_name** must be an alphanumeric string of 1 through 63 characters.

### Usage Guidelines

Use this command to define rule expressions to match destination port number in TCP headers.

### Examples

The following command defines a rule expression to match destination port number 10 in TCP headers:

```
tcp dst-port = 10
```
tcp duplicate

This command allows you to define rule expressions to match TCP retransmissions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

*active-charging service service_name > ruledef ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax Description**

```
| no | tcp duplicate operator condition |
```

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

*operator* must be one of the following:

- `!=`: Does not equal
- `=`: Equals

**condition**
Specifies the condition to match.

*condition* must be one of the following:

- **FALSE**: Not duplicated/retransmitted
- **TRUE**: Duplicated/retransmitted

**Usage Guidelines**
Use this command to specify rule expressions to match TCP retransmission.
Examples

The following command defines a rule expression to match TCP retransmissions:

tcp duplicate = TRUE
tcp either-port

This command allows you to define rule expressions to match either a destination or source port number in TCP headers.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
| no | tcp either-port \{ operator port_number \| \{ !range \| range \} \{ start_range to end_range \| port-map port_map_name \} \}

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- <=: Lesser 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_name
Specifies the port map for the port range. port_map_name must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines
Use this command to define rule expressions to match either a destination or source port number in TCP headers.
This command expression allows you to create a single ruledef using either-port, rather than needing two ruledefs (one with dst-port and one with src-port).

Examples
The following command defines a rule expression to match destination/source port number 10 in TCP header:
tcp either-port = 10
**tcp error**

This command allows you to define rule expressions to identify errors, either in the packet (for example, TCP checksum error) or in the TCP analyzer's Finite State Machine (FSM).

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

*active-charging service service_name > ruledef ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | tcp error operator condition
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- `!=`: Does not equal
- `=`: Equals

**condition**

Specifies the condition to match.

*condition* must be one of the following:

- `FALSE`
- `TRUE`

**Usage Guidelines**

Use this command to define a rule expression to identify errors, either in the packet (for example, TCP checksum error) or in the TCP analyzer's FSM.
The following command defines a rule expression to match TCP errors:

tcp error = TRUE
**tcp flag**

This command allows you to define rule expressions to match bit within the flag field of TCP headers.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

\[
\text{no | tcp flag operator flag}
\]

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - **operator** must be one of the following:
    - ![contains]: Does not contain
    - **contains**: Contains
    - ![=]: Does not equal
    - **=**: Equals

- **flag**
  - Specifies the flag value to match.
  - **flag** must be one of the following:
    - **ack**: TCP FLAG ACK
    - **fin**: TCP FLAG FIN
    - **push**: TCP FLAG PUSH
• **reset**: TCP FLAG RESET
• **syn**: TCP FLAG SYN

**Usage Guidelines**
Use this command to define rule expressions to match a bit within the flag field of TCP headers.

**Examples**
The following command defines a rule expression to match `reset` within flag field of TCP headers:
```
tcp flag = reset
```
tcp initial-handshake-lost

This command allows you to define rule expressions to match data packets when there has been no TCP handshaking to establish TCP connection.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax Description**

```
| no | tcp initial-handshake-lost operator condition
```

*no*
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.
`operator` must be one of the following:

- `!=`: Does not equal
- `=`: Equals

**condition**
Specifies the condition to match.
`condition` must be one of the following:

- `FALSE`
- `TRUE`

**Usage Guidelines**
Use this command to define rule expressions to match data packets when there has been no TCP handshaking to establish TCP connection.
The following command defines a rule expression to identify TCP flow where the initial handshake was not seen:

tcp initial-handshake-lost = TRUE
**tcp payload**

This command allows you to define rule expressions to match hexadecimal or ASCII string content in the payload protocol-signature field of the TCP payload.

- **Product**: ACS
- **Privilege**: Security Administrator, Administrator
- **Command Modes**: Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] tcp payload starts-with { hex-signature hex_string | string-signature string }
```

- **no**: If previously configured, deletes the specified rule expression from the current ruledef.

- **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 an alphanumerical string of 1 through 32 characters.

**Usage Guidelines**

Use this command to define rule expressions to match for Hex/ASCII string content in payload protocol-signature field.

This rule expression is useful for detecting certain applications.

**Examples**

The following command defines a rule expression to identify user traffic based on TCP protocol signature `tcp1`:

```
tcp payload starts-with string-signature tcp1
```
**tcp payload-length**

This command allows you to define rule expressions to match the length of a TCP payload.

<table>
<thead>
<tr>
<th>Product</th>
<th>ACS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

**Command Modes**

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**

```
| no | tcp payload-length operator payload_length
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  ```
  operator must be one of the following:
  - !=: Does not equal
  - <=: Lesser than or equals
  - ==: Equals
  - >=: Greater than or equals
  ```

- **payload_length**
  
  Specifies the TCP payload length to match.

  ```
  payload_length must be an integer from 0 through 40000000.
  ```

**Usage Guidelines**

Use this command to define rule expressions to match length of TCP payload, excluding the TCP or lower layer headers.

To match TCP control packets configure a payload-length of 0 (zero).
**Examples**

The following command defines a rule expression to match TCP payload length of 10000:

```
tcp payload-length = 10000
```
tcp previous-state

This command allows you to define rule expressions to match previous state of TCP connections.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**
| no | tcp previous-state operator tcp_previous_state |

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

- `!=`: Does not equal
- `=`: Equals

**tcp_previous_state**
Specifies the previous state to match.

tcp_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 Guidelines
Use this command to define rule expressions to match a TCP previous state.

Examples
The following command defines a rule expression to match user traffic based on previous state time-wait:
tcp previous-state = time-wait
tcp proxy-prev-state

This command allows you to define rule expressions to match TCP previous state on the ingress side of the TCP proxy.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**
```
| no | tcp proxy-prev-state operator previous_state
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  
  - !=: Does not equal
  - ==: Equals

- **previous_state**
  Specifies the previous state to match.
  
  - close
  - close-wait
  - closing
  - established
  - fin-wait1
• fin-wait2
• last-ack
• listen
• syn-received
• syn-sent
• time-wait

Usage Guidelines
If there is no TCP proxy configured, this configuration is not applicable.

For proxy-enabled flows, TCP state handling interprets the ingress side as the radio side and the egress side as the Internet side of the TCP connection.

tcp state and tcp prev-state is the state of the client stack, which would be either the state of the subscriber's stack (if flow is not proxy enabled) or the MS state of proxy on the egress-side (if flow is proxy-enabled).

tcp proxy-state and tcp proxy-prev-state is the state of the embedded TCP proxy server, that is the proxy ingress-side.

So, depending on the use case, if using tcp state and tcp prev-state an existing configuration may work fine regardless of whether proxy is enabled. For other use cases, other ruledefs may have to be created.

Both tcp state and tcp proxy-state can be used in the same ruledef. If proxy was being used, they would map to the egress-side and ingress-side, respectively. If proxy was not being used, then this would not match ruledef because proxy state would not be applicable.

Examples
The following command defines a rule expression to match user traffic based on TCP proxy previous state of established:

tcp proxy-prev-state = established
tcp proxy-state

This command allows you to define rule expressions to match the TCP state on the ingress side of the TCP proxy.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**active-charging service** service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

```
| no | tcp proxy-state operator state
```

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

**operator** must be one of the following:

- !=: Does not equal
- ==: Equals

**state**
Specifies the state to match.

**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 Guidelines**

If there is no TCP proxy configured, this configuration is not applicable.

For proxy-enabled flows, TCP state handling interprets the ingress side as the radio side and the egress side as the Internet side of the TCP connection.

`tcp state` and `tcp prev-state` is the state of the client stack, which would be either the state of the subscriber's stack (if flow is not proxy enabled) or the MS state of proxy on egress-side (if flow is proxy-enabled).

`tcp proxy-state` and `tcp proxy-prev-state` is the state of the embedded TCP proxy server, that is the proxy ingress-side.

So, depending on the use case, if using `tcp state` and `tcp prev-state` an existing configuration may work fine regardless of whether proxy is enabled. For other use cases, other ruledefs may have to be created.

Both `tcp state` and `tcp proxy-state` can be used in the same ruledef. If proxy was being used, they would map to the egress-side and ingress-side, respectively. If proxy was not being used, then this would not match the ruledef because proxy state would not be applicable.

**Examples**

The following command defines a rule expression to match user traffic based on TCP proxy previous state of established:

```
tcp proxy-state = established
```
**tcp server-port**

This command allows you to define rule expressions to match server port number in TCP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | tcp server-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map_name } }
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!`: Does not equal
  - `<` : Lesser 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_name**
Specifies the port map for the port range. port_map_name must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**
Use this command to define rule expressions to match server port number in TCP headers.

**Examples**
The following command defines a rule expression to analyze user traffic matching TCP server port 10:

tcp server-port = 10
**tcp session-length**

This command allows you to define rule expressions to match the total length of a TCP session.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | tcp session-length operator session_length
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `==`: Equals
- `>=`: Greater than or equals

**session_length**

Specifies the TCP session length (in bytes) to match as an integer from 0 through 4000000000.

**Usage Guidelines**

Use this command to define rule expressions to match the total length of a TCP session. The session-length is calculated by adding together the TCP payload-length values of all relevant packets.
Examples

The following command defines a rule expression to match user traffic based on TCP session length of 2000 bytes:

tcp session-length = 2000
tcp src-port

This command allows you to define rule expressions to match source a port number in TCP headers.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
| no | tcp src-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map_name } } |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
  • !=: Does not equal
  • <=: Lesser 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_name**
Specifies the port map for the port range. **port_map_name** must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**
Use this command to define rule expressions to match source a port number in TCP headers.

**Examples**
The following command defines a rule expression to analyze user traffic matching TCP source port 10:
```
tcp src-port = 10
```
tcp state

This command allows you to define rule expressions to match current state of TCP connections.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
| no | tcp state operator current_state |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- ==: Equals

current_state
Specifies the current state to match.
current_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 Guidelines
Use this command to define rule expressions to match a current state of TCP connections.

Examples
The following command defines a rule expression to match user traffic based on current state close:
```
tcp state = close
```
**tcp uplink**

This command allows you to define rule expressions to match uplink (subscriber to network) TCP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

```
| no | tcp uplink operator condition |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - **operator** must be one of the following:
    - !=: Does not equal
    - ==: Equals

- **condition**
  Specifies the condition.
  - **condition** must be one of the following:
    - FALSE
    - TRUE

**Usage Guidelines**
Use this command to define rule expressions to uplink TCP packets.
Examples

The following command defines a rule expression to uplink TCP packets:

tcp uplink = TRUE
tethering-detection

This command allows you to define rule expressions to match tethered or non-tethered flows.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description

tethering-detection [ip-ttl | os-ua] {flow-not-tethered | flow-tethered}
no tethering-detection

no
Deletes the tethering detection configuration from the ruledef.

ip-ttl
Specifies to select flows that were tethered or non-tethered as per IP-TTL values.

os-ua
Specifies to select flows that were tethered or non-tethered as per OS-UA lookups.
In 18 and later releases, IPv6 OS-based tethering detection is supported.

flow-not-tethered
Specifies to match if tethering is not detected on flow.

flow-tethered
Specifies to match if tethering is detected on flow.

Usage Guidelines

Use this command to define rule expressions to match tethered/non-tethered flows.

Note that in order for the rule containing the tethering-detection configuration to get matched, at least one valid rule line has to be present in it.
This configuration is treated in a special manner by the rule matching engine in that it is excluded from the condition **multi-line-or all-lines**. For example, if there are three rule-lines in a ruledef and multi-line-or is enabled as follows:

```plaintext
ruledef all-tethered-web-traffic
  http any-match = TRUE
  wsp any-match = TRUE
  multi-line-or all-lines
  tethering-detection flow-tethered
  exit
```

In this case, if for a packet only the rule line **tethering-detection flow-tethered** matches, it is not sufficient to result in a rule match even though **multi-line-or all-lines** is enabled in the ruledef.

**Examples**

The following command defines a rule expression to match tethered flows:

```plaintext
tethering-detection flow-tethered
```
**tftp any-match**

This command allows you to define rule expressions to match all Trivial File Transfer Protocol (TFTP) packets.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**  

```
| no | tftp any-match operator condition
```

**no**  
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**  
Specifies how to match.

```
operator must be one of the following:
- !=: Does not equal
- =: Equals
```

**condition**  
Specifies the condition to match.

```
condition must be one of the following:
- FALSE: Not analyzed
- TRUE: Analyzed
```

**Usage Guidelines**  
Use this command to define rule expressions to match all TFTP packets.
Examples

The following command defines a rule expression to match all TFTP packets:

```plaintext
tftp any-match = TRUE
```
**tftp data-any-match**

This command allows you to define rule expressions to match all TFTP data packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name (config-acs-ruledef)#
```

**Syntax Description**

```
| no | tftp data-any-match operator condition |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - **operator** must be one of the following:
    - \(!=\): Does not equal
    - \(=\): Equals

- **condition**
  Specifies the condition to match.
  - **condition** must be one of the following:
    - **FALSE**: Not analyzed
    - **TRUE**: Analyzed

**Usage Guidelines**
Use this command to define rule expressions to match all TFTP data packets.
Examples

The following command defines a rule expression to match all TFTP data packets:

```
tftp data-any-match = TRUE
```
This command allows to configure TLS/SSL Server Name Indication (SNI) and corresponding custom defined protocol (CDP).

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration


active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs-ruledef) #

**Syntax Description**

```bash
| no | tls { set-app-proto cdp_name_string | sni operator server_name_string } |
```

**no**
If previously configured, deletes the configuration in the current ruledef.

**set-app-proto cdp_name_string**
Specifies the name of the custom defined protocol (CDP) for TLS/SSL flows matching the ruledef. `cdp_name_string` must be an alphanumeric string of 1 through 19 characters.

**sni operator server_name_string**
Specifies the TLS/SSL Server Name Indication (SNI) field value in the Client Hello packet. `operator`: Specifies how to match and must be one of the following:

- `!`: Does not equal
- `=`: Equals
- `contains`: Contains
- `ends-with`: Ends with
- `starts-with`: Starts with

`server_name_string`: Specifies the server name and must be an alphanumeric string of 1 through 127 characters.
Usage Guidelines

Use this command to configure the TLS/SSL SNI and corresponding CDP. The CDP name for a TLS/SSL flow must match a set of SNI rule lines in multiline-and or multiline-or manner.

Examples

The following command configures the SNI to facebook.com:
```
tls sni = facebook.com
```

The following command configures the name of the corresponding protocol to facebook:
```
tls set-app-proto facebook
```
udp any-match

This command allows you to define rule expressions to match all UDP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[llocal]host_name(config-acs-ruledef)#

Syntax Description
| no | udp any-match operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

condition
Specifies the condition to match.
condition must be one of the following:
• FALSE
• TRUE

Usage Guidelines
Use this command to define rule expressions to match all UDP packets.
Examples

The following command defines a rule expression to match all UDP packets:

```
udp any-match = TRUE
```
**udp client-port**

This command allows you to define rule expressions to match client port number in UDP headers.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | udp client-port { operator port_number | !range | range } { start_range to end_range | port-map port_map_name } }
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - **operator** must be one of the following:
    - !=: Does not equal
    - <=: Lesser 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_name**

Specifies the port map for the port range. `port_map_name` must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to define rule expressions to match client port number in UDP headers.

**Examples**

The following command defines a rule expression to analyze user traffic matching UDP client port 500:

`udp client-port = 500`
udp downlink

This command allows you to define rule expressions to match downlink (network to subscriber) UDP packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | udp downlink operator condition

no

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

- operator must be one of the following:
  - =: Equals

**condition**

Specifies the condition to match.

- condition must be one of the following:
  - FALSE
  - TRUE

**Usage Guidelines**

Use this command to define rule expressions to match downlink UDP packets.
Examples

The following command defines a rule expression to match downlink UDP packets:

```
udp downlink = TRUE
```
**udp dst-port**

This command allows you to define rule expressions to match destination port number in UDP headers.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] udp dst-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map_name } }
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `<=`: Lesser 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

\textit{start\_range} to \textit{end\_range}

Specifies the starting and ending port numbers for the port range.

• \textit{start\_range} must be an integer from 1 through 65535.
• \textit{end\_range} must be an integer from 1 through 65535, and must be greater than \textit{start\_range}.

\textit{port-map \textit{port\_map\_name}}

Specifies the port map for the port range. \textit{\textit{port\_map\_name}} must be an alphanumeric string of 1 through 63 characters.

\textbf{Usage Guidelines}

Use this command to define rule expressions to match destination port number in UDP headers.

\textbf{Examples}

The following command defines a rule expression to match user traffic based on destination port number 10:

\texttt{udp dst-port = 10}
udp either-port

This command allows you to define rule expressions to match either a destination or source port number in UDP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] udp either-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map_name } }
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser 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_name**

Specifies the port map for the port range. *port_map_name* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to define rule expressions to match either destination or source port number in UDP headers.

**Examples**

The following command defines a rule expression to match user traffic based on match either source/destination port number 10:

```
udp either-port = 10
```
udp payload starts-with

This command allows you to define rule expressions to match hex/ASCII string content in UDP payload protocol-signature field.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax Description**

```
| no | udp payload starts-with { hex-signature hex_string | string-signature string }
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **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 an alphanumeric string of 1 through 32 characters.

**Usage Guidelines**

Use this command to define rule expressions to match for Hex/ASCII string content in UDP payload protocol-signature field.

This rule expression is useful for detecting certain applications.

**Examples**

The following command defines a UDP rule expression to analyze user traffic based on UDP protocol signature *udp1*:

```
udp payload starts-with string-signature udp1
```
udp server-port

This command allows you to define rule expressions to match server port number in UDP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**active-charging service service_name > ruledef ruledef_name**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | udp server-port { operator port_number | !range | range } { start_range to end_range | port-map port_map_name } |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  *operator* must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser 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_name**
Specifies the port map for the port range. **port_map_name** must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**
Use this command to define rule expressions to match source a server port number in UDP headers.

**Examples**
The following command defines a rule expression to analyze user traffic matching UDP server port 53:
```plaintext
udp server-port = 53
```
udp src-port

This command allows you to define rule expressions to match source port number in UDP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | udp src-port { operator port_number | !range | range } { start_range to end_range | port-map port_map_name } |

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- <=: Lesser 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_name**
Specifies the port map for the port range. *port_map_name* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**
Use this command to define rule expressions to match source port number in UDP headers.

**Examples**
The following command defines a rule expression to match source port number 10 in UDP headers:

```
udp src-port = 10
```
udp uplink

This command allows you to define rule expressions to match uplink (subscriber to network) UDP packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | udp uplink operator condition |
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  `operator` must be one of the following:

  - `=`: Equals

- **condition**
  
  Specifies the condition to match.

  `condition` must be one of the following:

  - `FALSE`
  - `TRUE`

**Usage Guidelines**

Use this command to define rule expressions to match uplink UDP packets.
Examples

The following command defines a rule expression to match uplink (from subscriber) UDP packets:

```
udp uplink = TRUE
```
wsp any-match

This command allows you to define rule expressions to match all Wireless Session Protocol (WSP) packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] wsp any-match operator condition
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

`operator` must be one of the following:

- `!=`: Does not equal
- `==`: Equals

**condition**

Specifies the condition to match.

`condition` must be one of the following:

- `FALSE`
- `TRUE`

**Usage Guidelines**

Use this command to specify a rule expression to match all WSP packets.
The following command defines a rule expression to match all WSP packets:

```
wsp any-match = TRUE
```
wsp content type

This command allows you to define rule expressions to match the content type field in WSP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

| no | wsp content type | case-sensitive | operator content_type |

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  * operator must be one of the following:
    * `!` (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 content type to match.

`content_type` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match "content type" field in WSP headers.

**Examples**

The following command defines a rule expression to WSP content type `test`:

```
wsp content type = test
```
**wsp domain**

This command allows you to define rule expressions to match domain portion of the URI for WSP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

```bash
[ no ] wsp domain [ case-sensitive ] operator domain
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  **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

**active-charging service service_name > ruledef ruledef_name**

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```
domain

Specifies the domain to match.

domain must be an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to define rule expressions to match the domain portion of URIs in WSP packets. From the URL, after http:// (if present) is removed, everything until the first "/" is the domain.

Examples

The following command defines a rule expression to match user traffic based on domain name testdomain:

wsp domain = testdomain
**wsp downlink**

This command allows you to define rule expressions to match downlink (network to subscriber) WSP packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] wsp downlink operator condition
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**condition**

Specifies the downlink (from the Mobile Node direction) status to match.

**Usage Guidelines**

Use this command to define rule expressions to match downlink WSP packets.
Examples

The following command defines a rule expression to match downlink WSP packets:

```
wsp downlink = TRUE
```
**wsp first-request-packet**

This command allows you to define rule expressions to match WSP first-request-packet.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

```
[no] wsp first-request-packet operator condition
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `=`: Equals

- **condition**
  - Specifies the condition to match.
  - `condition` must be one of the following:
    - `FALSE`
    - `TRUE`

**Usage Guidelines**

Use this command to define rule expressions to match the GET or POST request, if it is the first WSP request for the subscriber's session.
Examples

The following command defines a rule expression to match WSP first-request-packet:

```
wsp first-request-packet = TRUE
```
wsp host

This command allows you to define rule expressions to match the host name header field in WSP headers.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | wsp host | case-sensitive | operator host_name |

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.

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**

Specifies the WSP host name to match.

*host_name* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match host name header field in WSP headers.

**Examples**

The following command defines a rule expression to match host name *host1* in WSP headers:

```plaintext
wsp host contains host1
```
wsp pdu-length

This command allows you to define rule expressions to match WSP PDU length.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef) #

**Syntax Description**

| no | wsp pdu-length operator pdu_length |

no

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**operator** must be one of the following:

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `=`: Equals
- `>=`: Greater than or equals

**pdu_length**

Specifies the WSP PDU length (in bytes) to match.

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

**Usage Guidelines**

Use this command to define rule expressions to match WSP PDU length (header + payload) in bytes.
Examples

The following command defines a rule expression to match user traffic based on WSP PDU length of 10000 bytes:

```
wsp pdu-length = 10000
```
**wsp pdu-type**

This command allows you to define rule expressions to match WSP PDU type in the current packet.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

```
(no) wsp pdu-type operator pdu_type
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!`: Does not equal
    - `=`: Equals

- **pdu_type**
  - Specifies the WSP PDU type to match.
  - `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 Guidelines
Use this command to define rule expressions to match WSP PDU type value in current packet.

Examples
The following command defines a rule expression to match WSP PDU type resume:
```
wsppdu-type resume
```
**wsp previous-state**

This command allows you to define rule expressions to match previous WSP method invocation state.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

```
[ no ] wsp previous-state operator wsp_previous_state
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator must be one of the following:*

- `!=`: Does not equal
- `=`: Equals

**wsp_previous_state**

Specifies the previous state to match.

*wsp_previous_state must be one of the following:*

- `init`
- `response-error`
- `response-ok`
- `waiting-for-response`
Usage Guidelines

Use this command to define rule expressions to match WSP previous state.

Examples

The following command defines a rule expression to match WSP previous state of `response-ok`:

```
wsprev = response-ok
```
**wsp reply code**

This command allows you to define rule expressions to match WSP reply code.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

```
[ no ] wsp reply code operator reply_code
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  **operator** must be one of the following:

  - !=: Does not equal
  - <=: Lesser than or equals
  - =: Equals
  - >=: Greater than or equals

- **reply_code**
  
  Specifies the WSP reply code to match.

  **reply_code** must be an integer from 0 through 101.

**Usage Guidelines**

Use this command to define rule expressions to match WSP reply code.
wsp reply code

**Examples**

The following command defines a rule expression to match WSP reply code of 50:

```
wsp reply code = 50
```
wsp session-length

This command allows you to define rule expressions to match total length of a WSP session.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | wsp session-length operator session_length |

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- <=: less than equals
- =: Equals
- >=: greater than equals

session_length

Specifies the WSP session length (in bytes) to match.

session_length must be an integer from 1 through 65535.

Usage Guidelines

Use this command to define rule expressions to match total length of WSP session.
Examples

The following command defines a rule expression to match WSP session length of 2000 bytes:

```
ws session-length = 2000
```
**wsp session-management**

This command allows you to define rule expressions to match WSP Session Management state.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

| no | wsp session-management { previous-state | state } operator state |

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **previous-state**
  Specifies the previous WSP Session Management state.

- **state**
  Specifies current WSP Session Management Finite State Machine (FSM) state.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **state**
  Specifies the state to match.
  For `previous-state`, `state` must be one of the following:
For state, state must be one of the following:

- close
- connected
- connecting
- init
- resuming
- suspended

**Usage Guidelines**
Use this command to define rule expressions to match a WSP Session Management state.

**Examples**
The following command defines a rule expression to match previous WSP Session Management state of connecting:

```
wsp session-management previous-state = connecting
```
**wsp state**

This command allows you to define rule expressions to match WSP Method Invocation state.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**active-charging service service_name > ruledef ruledef_name**

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | wsp state operator current_state
```

*no*

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- `!=`: Does not equal
- `=`: Equals

**current_state**

Specifies the current state to match.

*current_state* must be one of the following:

- `close`
- `response-error`
- `response-ok`
- `waiting-for-response`
Usage Guidelines

Use this command to define rule expressions to match WSP Method Invocation state.

Examples

The following command defines a rule expression to match a WSP Method Invocation state `close`:

```
wsp state = close
```
wsp status

This command has been deprecated. See the wsp reply-code command.
**wsp tid**

This command allows you to define rule expressions to match Transaction Identifier (TID) field for connection-less WSP.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

**active-charging service service_name > ruledef ruledef_name**

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax Description**

```plaintext
[no] wsp tid operator transaction_id
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- `!=`: Does not equal
- `=`: Equals

**transaction_id**

Specifies the transaction identifier to match.

*transaction_id* must be an integer from 0 through 255.

**Usage Guidelines**

Use this command to define rule expressions to match TID field for connection-less WSP.

**Examples**

The following command defines a rule expression to match a TID value of 22 for connection-less WSP:

```plaintext
wsp tid = 22
```
wsp total-length

This command has been deprecated. See the **wsp session-length** command.
**wsp transfer-encoding**

This command allows you to define rule expressions to match transfer encoding present in WSP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**

```
| no | wsp transfer-encoding | case-sensitive | operator transfer_encoding |
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  - Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  - Specifies how to match.
  - **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
**transfer_encoding**

This must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to define rule expressions to match transfer encoding present in WSP header.

**Examples**

The following command defines a rule expression to match user traffic based on WSP transfer encoding 7:

```
wsp transfer-encoding contains 7
```
### wsp uplink

This command allows you to define rule expressions to match uplink (subscriber to network) WSP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**

```
| no | wsp uplink operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  Specifies the uplink (to the Mobile Node direction) status to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage Guidelines**

Use this command to define rule expressions to match uplink WSP packets.
Examples

The following command defines a rule expression to match uplink WSP packets:

```plaintext
wsp uplink = TRUE
```
**wsp url**

This command allows you to define rule expressions to match WSP URL.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

```
| no | wsp url | case-sensitive | operator url |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  *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
  - regex: Regular expression
• **starts-with**: Starts with

**url**

Specifies the URL to match.

*url* must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to define rule expressions to match the complete URL, including the host portion.

The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the *Enhanced Charging Service Administration Guide*.

**Table 12: Special Characters Supported in Regex Rule Expressions**

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
</tbody>
</table>
| ?               | Match zero or one character  
  **Important** The CLI does not support configuring "?" directly, you must instead use "\077".  
  For example, if you want to match the string "xyz<any one character>pqr", you must configure it as:  
  **http host regex** "xyz\077pqr"  
  In another example, if you want to exactly match the string "url?resource=abc", you must configure it as:  
  **http uri regex** "url\077resource=abc"  
  Where, the first "\" (backslash) is for the escaping of "?", and then "\077" for specifying "?" to the CLI. |
| \\character     | Escaped character |
| \?              | Match the question mark (\<ctrl-v>? character |
| \+              | Match the plus character |
| \*              | Match the asterisk character |
| \a              | Match the Alert (ASCII 7) character |
| \b              | Match the Backspace (ASCII 8) character |
| \f              | Match the Form-feed (ASCII 12) character |
| \n              | Match the New line (ASCII 10) character |
### Regex Character

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\r</td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td>\t</td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td>\v</td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td>\0</td>
<td>Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td>\</td>
<td>Match the backslash character</td>
</tr>
<tr>
<td>Bracketed range [0-9]</td>
<td>Match any single character from the range</td>
</tr>
<tr>
<td>A leading ^ in a range</td>
<td>Do not match any in the range. All other characters represent themselves.</td>
</tr>
<tr>
<td>\x##</td>
<td>Any ASCII character as specified in two-digit hex notation. For example, \x5A yields a &quot;Z&quot;.</td>
</tr>
<tr>
<td></td>
<td>Specify OR regular expression operator</td>
</tr>
</tbody>
</table>

**Important**

When using the regex operator "|" in regex expressions, always wrap the string in double quotes. For example, if you want to match the string "pqr" OR "xyz", you must configure it as:

```
http host regex "pqr|xyz"
```

### Examples

The following command defines a rule expression to match user traffic based on WSP URL.

```
wsp url = wsp://wiki.tcl.tk
```

The following command defines a regex rule expression to match any of the following or similar values in the WSP URL string:

```
wsp url regex "wsp://(dwld|opera|home.opera|dwld\[1-3\]).yahoo.com"
```
**wsp user-agent**

This command allows you to define rule expressions to match user agent field in WSP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | wsp user-agent | case-sensitive | operator user_agent |
```

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**case-sensitive**
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

**operator**
Specifies how to match.

*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 to match.

*user_agent* must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to define rule expressions to match a user agent field in WSP headers.

**Examples**

The following command defines a rule expression to match value `test` in user agent field in WSP headers:

```plaintext
wsp user-agent contains test
```
wsp x-header

This command allows you to define rule expressions to match WSP extension-headers (x-headers).

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
\[ no \] wsp x-header name [ case-sensitive ] [ operator string ]

no
If previously configured, deletes the specified rule expression from the current ruledef.

name
Specifies the x-header value as an alphanumeric string of 1 through 31 characters.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
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 as an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command 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 the RFC standard.

**Examples**

The following command defines a rule expression to analyze user traffic containing WSP extension-header of `test_field` and value of `test_string`:

```
wspx x-header test_field = test_string
```
wtp any-match

This command allows you to define rule expressions to match all Wireless Transaction Protocol (WTP) packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] wtp any-match operator condition
```

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

`operator` must be one of the following:

- `!=`: Does not equal
- `=`: Equals

**condition**

Specifies the condition to match.

`condition` must be one of the following:

- `FALSE`
- `TRUE`

**Usage Guidelines**

Use this command to define rule expressions to match all WTP packets.
Examples

The following command defines a rule expression to match all WTP packets:

```bash
wtp any-match = TRUE
```
wtp downlink

This command allows you to define rule expressions to match downlink (network to subscriber) WTP packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | wtp downlink operator condition |
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `==`: Equals

- **condition**
  - Specifies the downlink (from the Mobile Node direction) status to match.
  - `condition` must be one of the following:
    - `FALSE`
    - `TRUE`

**Usage Guidelines**

Use this command to define rule expressions to match downlink WTP packets.
**Examples**

The following command defines a rule expression to match all downlink WTP packets:

```
wtp downlink = TRUE
```
wtp gtr

This command allows you to define rule expressions to match Group Transmission (GTR) flag in the current WTP PDU.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | wtp gtr operator condition |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- =: Equals

condition
Specifies the condition to match.

condition must be one of the following:

- FALSE
- TRUE

Usage Guidelines

Use this command to define rule expressions to match the GTR flag (that indicates the last packet of a packet group) in the current WTP PDU.
Examples

The following command defines a rule expression to match WTP user traffic based on WTP GTR:

```bash
wtp gtr = TRUE
```
wtp pdu-length

This command allows you to define rule expressions to match WTP PDU length.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > Ruledef Configuration

**Syntax Description**

```
[ no ] wtp pdu-length operator pdu_length
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  
  - `!=`: Does not equal
  - `=`: Equals

- **pdu_length**
  Specifies the WTP PDU length (in bytes) to match.
  
  `pdu_length` must be an integer from 1 through 65535.

**Usage Guidelines**  
Use this command to define rule expressions to match WTP PDU length (header + payload) in bytes.

**Examples**  
The following command defines a rule expression to match WTP PDU length of 9647 bytes:

```
wtp pdu-length = 9647
```
wtp pdu-type

This command allows you to define rule expressions to match WTP PDU type.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | wtp pdu-type operator pdu_type
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

- `!=`: Does not equal
- `==`: Equals

**pdu_type**

Specifies the WTP PDU type to match.

- `abort`
- `ack`
- `invoke`
- `negative-ack`
- `result`
Usage Guidelines
Use this command to define rule expressions to match WTP PDU type.

Examples
The following command defines a rule expression to match the WTP PDU type result:
```
wt pdu-type = result
```
wtp previous-state

This command allows you to define rule expressions to match previous WTP state.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]\host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | wtp previous-state operator wtp_previous_state
```

*no*

If previously configured, deletes the specified rule expression from the current ruledef.

*operator*

Specifies how to match.

*operator* must be one of the following:

- `!=`: Does not equal
- `=`: Equals

*wtp_previous_state*

Specifies the previous state to match.

*wtp_previous_state* must be one of the following:

- `ack-sent`
- `init`
- `invoke-sent`
- `rcvd`
- `result-rcvd`
Usage Guidelines

Use this command to define rule expressions to match WTP previous state.

Examples

The following command defines a rule expression to match user traffic based on WTP previous state of ack-sent:

```
wtpprevious-state = ack-sent
```
**wtp rid**

This command allows you to define rule expressions to match Re-transmission Indicator (RID) flag set in WTP traffic.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**
`[no] wtp rid operator condition`

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `==`: Equals

- **condition**
  - Specifies the condition to match.
  - `condition` must be one of the following:
    - `FALSE`
    - `TRUE`

**Usage Guidelines**
Use this command to define rule expressions to match WTP RID flag.
Examples

The following command defines a rule expression to match user traffic containing WTP RID flag:

```
wtprid = TRUE
```
**wtp state**

This command allows you to define rule expressions to match current WTP state.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | wtp state operator current_state
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- `!` or `!=`: Does not equal
- `=` or `==`: Equals

**current_state**

Specifies the current state to match.

*current_state* must be one of the following:

- `ack-sent`
- `close`
- `init`
- `invoke-sent`
- `rcvd`
Usage Guidelines

Use this command to define rule expressions to match current WTP state.

Examples

The following command defines a rule expression to match user traffic based on current WTP state close:

```
wtp state = close
```
**wtp tid**

This command allows you to define rule expressions to match WTP Transaction Identifier (TID).

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```plaintext
| no | wtp tid operator transaction_id
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  - **operator** must be one of the following:
    - `!=`: Does not equal
    - `==`: Equals

- **transaction_id**
  
  Specifies the transaction identifier to match.

  - `transaction_id` must be an integer from 0 through 65535.

**Usage Guidelines**

Use this command to define rule expressions to match WTP TID. This expression ignores the high order bit in the protocol that indicates the direction.

**Examples**

The following command defines a rule expression to match user traffic containing WTP TID value of 22:

```
wtp tid = 22
```
wtp transaction class

This command allows you to define rule expressions to match WTP Transaction Class (TCL) state.

Product
- ACS

Privilege
- Security Administrator, Administrator

Command Modes
- Exec > ACS Configuration > Ruledef Configuration
- active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef)#

Syntax Description

| no | wtp transaction class operator transaction_class |

no
- If previously configured, deletes the specified rule expression from the current ruledef.

operator
- Specifies how to match.

operator must be one of the following:
- !=: Does not equal
- ==: Equals

transaction_class
- Specifies the WTP TCL to match.

transaction_class must be an integer from 0 through 2.

Usage Guidelines
- Use this command to define rule expressions to match WTP transaction class.

Examples
- The following command defines a rule expression to match WTP traffic based on WTP transaction class 2:

  wtp transaction class = 2
wtp ttr

This command allows you to define rule expressions to match WTP Trailer Transmission (TTR) flag.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description
| no | wtp ttr operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

condition
Specifies the condition to match.
condition must be one of the following:
• FALSE
• TRUE

Usage Guidelines
Use this command to define rule expressions to match TTR flag (used to indicate the last packet in a segmented message) in the current WTP PDU.
Examples

The following command defines a rule expression to match WTP traffic based on the presence of the WTP TTR flag:

```
wtp ttr = TRUE
```
**wtp uplink**

This command allows you to define rule expressions to match uplink (subscriber to network) WTP packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | wtp uplink operator condition
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

**condition**

Specifies the condition to match.

**Usage Guidelines**

Use this command to define rule expressions to match uplink WTP packets.
The following command defines a rule expression to match all uplink WTP packets:

```
wtp uplink = TRUE
```
www any-match

This command allows you to define rule expressions to match all WWW packets. It is true for HTTP, WAP1.x, and WAP2.0 protocols.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | www any-match operator condition
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

* operator must be one of the following:

  * !=: Does not equal
  * =: Equals

**condition**

Specifies the condition to match.

* condition must be one of the following:

  * FALSE
  * TRUE

**Usage Guidelines**

Use this command to define rule expressions to match all WWW packets. This expression is true for HTTP, WAP1.x, and WAP2.0 protocols.
Examples

The following command defines a rule expression to match all WWW packets:

```
www any-match = TRUE
```
**www content type**

This command allows you to define rule expressions to match the Content-Type field of HTTP/WSP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**
```
| no | www content type | case-sensitive | operator content_type |
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  **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 value to match.

*content_type* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match the "content type" field of HTTP/WSP header.

**Examples**

The following command defines a rule expression to match the WWW content type *Accept*:

```plaintext
www content type = Accept
```
www domain

This command allows you to define rule expressions to match the domain portion of URIs in WSP/HTTP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax Description

| no | www domain | case-sensitive | operator | domain |

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
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
**domain**

Specifies the domain to match.

domain must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to define rule expressions to match the domain portion of URIs in WSP/HTTP packets. From the URL, after `http://` (if present) is removed, everything until the first `"/"` is the domain.

**Examples**

The following command defines a rule expression to match user traffic based on domain name `testdomain`:

```
www domain = testdomain
```
**www downlink**

This command allows you to define rule expressions to match downlink (network to subscriber) HTTP/WSP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

```
active-chargingservice service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-acs-ruledef) #
```

**Syntax Description**

```
| no | www downlink operator condition
```

`no`
If previously configured, deletes the specified rule expression from the current ruledef.

`operator`
Specifies how to match.
`operator` must be one of the following:

- `!=`: Does not equal
- `=`: Equals

`condition`
Specifies the condition to match.
`condition` must be one of the following:

- `FALSE`
- `TRUE`

**Usage Guidelines**
Use this command to define rule expressions to match downlink HTTP/WSP packets.
Examples

The following command defines a rule expression to match all downlink WWW packets:

```
www downlink = TRUE
```
www first-request-packet

This command allows you to define rule expressions to match the GET or POST request, if it is the first WSP/HTTP request for the subscriber's session.

Product  
ACS

Privilege  
Security Administrator, Administrator

Command Modes  
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

(local)host_name(config-acs-ruledef)#

Syntax Description

| no | www first-request-packet operator condition |

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• ==: Equals

condition

Specifies the condition to match.

condition must be one of the following:

• FALSE
• TRUE

Usage Guidelines

Use this command to define rule expressions to match the GET or POST request, if it is the first WSP/HTTP request for the subscriber's session.
Examples

The following command defines a rule expression to match user traffic based on the WWW first-request-packet:

```plaintext
www first-request-packet = TRUE
```
**www header-length**

This command allows you to define rule expressions to match WWW packet header length.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
| no | www header-length operator header_length
```

`no`
If previously configured, deletes the specified rule expression from the current ruledef.

`operator`
Specifies how to match.

`operator` must be one of the following:

- `!`: Does not equal
- `<=`: Lesser than or equals
- `=`: Equals
- `>=`: Greater than or equals

`header_length`
Specifies the WWW packet header length (in bytes) to match, `header_length` must be an integer from 0 through 65535.

**Usage Guidelines**
Use this command to define rule expressions to match WWW packet header length.
Examples

The following command defines a rule expression to match user traffic based on WWW packet header length of 10000 bytes:

```
www header-length = 10000
```
www host

This command allows you to define rule expressions to match the "host name" header field present in HTTP/WSP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs-ruledef) #

Syntax Description

| no | www host | case-sensitive | operator host_name |

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.

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**

Specifies the WWW host name to match.

*host_name* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match the host name header field present in HTTP/WSP headers.

**Examples**

The following command defines a rule expression to match user traffic based on WWW host name *host1*:

```
www host = host1
```
www payload-length

This command allows you to define rule expressions to match WWW payload length.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Ruledef Configuration
  active-charging service service_name > ruledef ruledef_name
Entering the above command sequence results in the following prompt:
  [local] host_name (config-acs-ruledef)#

Syntax Description

| no | www payload-length operator payload_length |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• <=: Lesser than or equals
• =: Equals
• >=: Greater than or equals

payload_length
Specifies the payload length (in bytes) to match.
payload_length must be an integer from 1 through 4000000000.

Usage Guidelines Use this command to define rule expressions to match WWW payload length.
The following command defines a rule expression to match user traffic based on WWW payload length of 10000:

```plaintext
www payload-length = 10000
```
**www pdu-length**

This command allows you to define rule expressions to match WWW PDU length.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```plaintext
| no | www pdu-length operator pdu_length
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

- `!=`: Does not equal
- `<=`: Less than or equals
- `==`: Equals
- `>=`: Greater than or equals

**pdu_length**

Specifies the WWW PDU length (in bytes) to match.

*pdu_length* must be an integer from 0 through 65535.

**Usage Guidelines**

Use this command to define rule expressions to match WWW PDU length (header + payload) in bytes.
Examples

The following command defines a rule expression to match user traffic based on WWW PDU length of 9767 bytes:

\texttt{www pdu-length = 9767}
**www previous-state**

This command allows you to define rule expressions to match previous HTTP/WSP(HTTP) state.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

| no | www previous-state operator www_previous_state |

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

*operator* must be one of the following:

- !=: Does not equal
- =: Equals

**www_previous_state**

Specifies the previous state to match.

*www_previous_state* must be one of the following:

- init
- response-error
- response-ok
- waiting-for-response
Usage Guidelines

Use this command to define rule expressions to match a previous HTTP/WSP(HTTP) state.

Examples

The following command defines a rule expression to match user traffic based on WWW previous state init:

```plaintext
www previous-state = init
```
www reply code

This command allows you to define rule expressions to match WWW reply code arguments.

Product  ACS

Privilege  Security Administrator, Administrator

Command Modes  Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax Description  | no | www reply code operator reply_code

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

reply_code

Specifies the reply code to match.
reply_code must be an integer from 100 through 599.

Usage Guidelines  Use this command to define rule expressions to match HTTP 1.1 status code, or WSP status code that has been remapped to the corresponding HTTP value.
WSP status codes 0 – 101 are automatically remapped to the HTTP status code values, as defined by Table 36 WAP-230-WSP Version 5.

Examples

The following command defines a rule expression to analyze WWW user traffic based on reply code of 125:

```
www reply code = 125
```
www state

This command allows you to define rule expressions to match current HTTP/WSP(HTTP) state.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local] host_name(config-acs-ruledef)#

Syntax Description

| no | www state operator current_state |

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• =: Equals

current_state
Specifies the current state to match.
current_state must be one of the following:

• close
• response-error
• response-ok
• waiting-for-response
**Usage Guidelines**

Use this command to define rule expressions to match current HTTP/WSP state.

**Examples**

The following command defines a rule expression to match user traffic based on the current WWW state:

```plaintext
close:
www state = close
```
www transfer-encoding

This command allows you to define rule expressions to match the transfer encoding field present in HTTP/WSP(HTTP) headers.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax Description**

| no | www transfer-encoding | case-sensitive | operator transfer_encoding |

*no*

If previously configured, deletes the specified rule expression from the current ruledef.

*case-sensitive*

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

*operator*

Specifies how to match.

*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
**transfer_encoding**

Specifies the WWW transfer encoding to match.

*transfer_encoding* must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match the "transfer encoding" field present in HTTP/WSP (HTTP) headers.

**Examples**

The following command defines a rule expression to match user traffic based on the WWW transfer encoding *user1*:

```
www transfer-encoding = user1
```
This command allows you to define rule expressions to match URL for any Web protocol analyzer—HTTP, WAP1.X, WAP2.0.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax Description**

```
[ no ] www url [ case-sensitive ] operator url
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  - Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  - Specifies how to match.

  - **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
    - regex: Regular expression
• **starts-with**: Starts with

`url`

Specifies the URL to match.

`url` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

**Usage Guidelines**

Use this command to define rule expressions to match the URL for any Web protocol analyzer—HTTP, WAP1.X, WAP2.0.

The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the *Enhanced Charging Service Administration Guide*.

**Table 13: Special Characters Supported in Regex Rule Expressions**

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>?</td>
<td>Match zero or one character</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> The CLI does not support configuring &quot;?&quot; directly, you must instead use &quot;\077&quot;. For example, if you want to match the string &quot;xyz&lt;any one character&gt;pqr&quot;, you must configure it as:</td>
</tr>
<tr>
<td>http host regex</td>
<td>&quot;xyz\077pqr&quot;</td>
</tr>
<tr>
<td></td>
<td>In another example, if you want to exactly match the string &quot;url?resource=abc&quot;, you must configure it as:</td>
</tr>
<tr>
<td>http uri regex</td>
<td>&quot;url\077resource=abc&quot;</td>
</tr>
<tr>
<td></td>
<td>Where, the first &quot;\&quot; (backslash) is for the escaping of &quot;?&quot;, and then &quot;\077&quot; for specifying &quot;?&quot; to the CLI.</td>
</tr>
<tr>
<td>\</td>
<td>Escaped character</td>
</tr>
<tr>
<td>?</td>
<td>Match the question mark (&lt;ctrl-v&gt;&gt;?) character</td>
</tr>
<tr>
<td>+</td>
<td>Match the plus character</td>
</tr>
<tr>
<td>*</td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td>\a</td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td>\b</td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td>\f</td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
<tr>
<td>\n</td>
<td>Match the New line (ASCII 10) character</td>
</tr>
<tr>
<td>Regex Character</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>\r</td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td>\t</td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td>\v</td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td>\0</td>
<td>Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td>&quot;</td>
<td>Match the backslash character</td>
</tr>
</tbody>
</table>

Bracketed range [0-9] Match any single character from the range

A leading ^ in a range Do not match any in the range. All other characters represent themselves.

\x## Any ASCII character as specified in two-digit hex notation.
For example, \x5A yields a "Z".

<table>
<thead>
<tr>
<th></th>
<th>Specify OR regular expression operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important</td>
<td>When using the regex operator &quot;</td>
</tr>
<tr>
<td></td>
<td>For example, if you want to match the string &quot;pqr&quot; OR &quot;xyz&quot;, you must configure it as:</td>
</tr>
<tr>
<td>http host regex</td>
<td>&quot;pqr</td>
</tr>
</tbody>
</table>

Examples

The following command defines a rule expression to match user traffic based on WWW URL www.abc.com:

www url = www.abc.com


www url regex
"http://(tp2.site.com|134.210.11.3)/httppvc_clnsssite.com.wap.symphonieserver.musicwaver.com/"
ACS Service Scheme Configuration Mode

Commands

The ACS Service Scheme Configuration Mode is used to enable the association of service-scheme based on subscriber class.

**Command Modes**

Exec > ACS Configuration > ACS Service Scheme Configuration

```
active-charging service service_name > service-scheme service_scheme_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-servscheme)#
```

---

**Important**

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

- end, page 1416
- exit, page 1417
- trigger, page 1418
**end**

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

**Usage Guidelines**
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 Description**
exit

**Usage Guidelines**
Use this command to return to the parent configuration mode.
trigger

This command allows you to specify the trigger that needs to be handled for the associated service-scheme.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > ACS Configuration > ACS Service Scheme Configuration

*active-charging service service_name > service-scheme service_scheme_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-servscheme)#
```

**Syntax Description**  

```
| no | trigger { loc-update | sess-setup }
```

- **no**  
  If previously configured, deletes the specified configuration.

- **loc-update | sess-setup**  
  Specifies the trigger action for service-scheme.

  - **loc-update**: Triggers whenever location changes for the subscriber
  - **sess-setup**: Triggers at session setup.

**Usage Guidelines**  

Use this command to configure trigger events such as session-setup and location-update that will be handled under the service-scheme.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-servscheme-trigger)#
```

Also see the *ACS Service Scheme Trigger Configuration Mode Commands* chapter.

**Examples**  

The following command is configured to define session setup event as an event type that will be handled in the service-scheme:

```
trigger sess-setup
```
ACS Service Scheme Trigger Configuration Mode

The ACS Service Scheme Trigger Configuration Mode is used to configure the set of triggers to be handled under the associated service-scheme.

**Command Modes**

Exec > ACS Configuration > ACS Service Scheme Configuration > ACS Service Scheme Trigger Configuration

```
active-charging service service_name > service-scheme service_scheme_name > trigger { loc-update | sess-setup }
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-servscheme-trigger)#
```

**Important**

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

- end, page 1420
- exit, page 1421
- priority, page 1422
**end**

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

end

**Usage Guidelines**

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 Description
exit

Usage Guidelines
Use this command to return to the parent configuration mode.
priority

This command allows you to assign priority to the trigger events in service-scheme.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > ACS Service Scheme Configuration > ACS Service Scheme Trigger Configuration

- active-charging service service_name > service-scheme service_scheme_name > trigger { flow-create | loc-update | sess-setup }

Entering the above command sequence results in the following prompt:

[local] host_name(config-servscheme-trigger)#

Syntax Description

- **priority** priority
  - Specifies the priority to be assigned to the trigger events.
  - **priority** must be an integer from 1 through 127.

- **trigger-condition** trigger_condn_name
  - Specifies the trigger condition definition.
  - **trigger_condn_name** must be an alphanumeric string of 1 through 63 characters.

- **trigger-action** trigger_action_name
  - Specifies the trigger action definition.
  - **trigger_action_name** must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

- Use this command to assign priority to the trigger events configured in service-scheme. The priority must be unique within a trigger.
Examples

The following command is configured to set priority as 10 with respective trigger condition tc1 and trigger action ta1:

```
priority 10 trigger-condition tc1 trigger-action ta1
```
priority
ACS Subscriber Base Configuration Mode

Commands

The ACS Subscriber Base Configuration Mode is used to configure Active Charging Service subscriber base.

```
Command Modes
Exec > ACS Configuration > ACS Subscriber Base Configuration
active-charging service service_name > subscriber-base subs_base_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-subscriber-base)#
```

### Important

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

- end, page 1426
- exit, page 1427
- priority, page 1428
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

**Usage Guidelines**
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 Description**

exit

**Usage Guidelines**

Use this command to return to the parent configuration mode.
priority

This command allows you to assign priority to the service-scheme association within a subscriber base.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > ACS Subscriber Base Configuration

active-charging service service_name > subscriber-base subs_base_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-subscriber-base)#

Syntax Description
priority priority subs-class subs_class_name bind service-scheme serv_scheme_name

no
If previously configured, deletes the specified configuration.

priority
Specifies the priority to be assigned to service-scheme.

priority must be an integer from 1 through 127.

subs-class subs_class_name
Specifies the subscriber class definition to a subscriber base.

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

bind
Specifies the association of service-scheme within subscriber class.

service-scheme serv_scheme_name
Specifies the service scheme definition.

serv_scheme_name must be an alphanumeric string of 1 through 63 characters.
**Usage Guidelines**

Use this command to assign priority to the service-scheme association within a subscriber base. This priority has to be unique within a subscriber base.

**Examples**

The following command is configured to set priority as 5 to associate service-scheme named ss1:

```
priority 5 subs-class sc1 bind service-scheme ss1
```
priority
ACS Subscriber Class Configuration Mode Commands

The ACS Subscriber Class Configuration Mode is used to configure Active Charging Service subscriber class.

**Command Modes**

Exec > ACS Configuration > ACS Subscriber Class Configuration

**active-charging service service_name > subs-class subs_class_name**

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-subsclass)#
```

**Important**

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

- any-match, page 1432
- apn, page 1433
- end, page 1434
- exit, page 1435
- multi-line-or, page 1436
- rulebase, page 1437
- v-apn, page 1438
any-match

This command is used to enable or disable the wildcard configuration.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > ACS Subscriber Class Configuration

active-charging service service_name > subs-class subs_class_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-subclass)#

Syntax Description  | no | any-match operator condition

no
If previously configured, deletes the specified configuration.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• =: Equals

condition
Specifies the condition to match.
condition must be one of the following:

• FALSE
• TRUE

Usage Guidelines Use this command to enable or disable the wildcard configuration.
This command allows you to specify the APN name as a condition.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > ACS Subscriber Class Configuration

active-charging service service_name > subs-class subs_class_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-acs-subsclass) #

Syntax Description

| no | apn operator apn_name

no
If previously configured, deletes the specified configuration.

operator
Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- ==: Equals

apn_name
Specifies the APN name.
apn_name must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines
Use this command to specify the APN name as a condition.

Examples
The following command configures an APN named xyz.com:
apn = xyz.com
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

**Usage Guidelines**
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 Description**

exit

**Usage Guidelines**

Use this command to return to the parent configuration mode.
multi-line-or

This command allows to check if the OR operator must be applied to all lines in a subscriber class.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > ACS Subscriber Class Configuration

`active-charging service service_name > subs-class subs_class_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-subsclass)#
```

**Syntax Description**

| | no | multi-line-or all-lines |

**Usage Guidelines**

Use this command to check if the OR operator must be applied to all lines in a subscriber class.
**rulebase**

This command allows you to specify the rule base name as a condition.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > ACS Subscriber Class Configuration

`active-charging service service_name > subs-class subs_class_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-subsclass)#
```

**Syntax Description**

```
[ no ] rulebase operator rulebase_name
```

- **no**
  If previously configured, deletes the specified configuration.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **rulebase_name**
  Specifies the rule base name.
  `rulebase_name` must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to specify the rule base name as a condition.

**Examples**

The following command configures a rule base named `plan1`:

```
rulebase = plan1
```
v-apn

This command allows you to specify the virtual APN name as a condition.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > ACS Subscriber Class Configuration

active-charging service service_name > subs-class subs_class_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-subsclass)#

Syntax Description

| no | v-apn operator v_apn_name

no
If previously configured, deletes the specified configuration.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• =: Equals

v_apn_name
Specifies the virtual APN name.
v_apn_name must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines
Use this command to specify the virtual APN name as a condition.

Examples
The following command configures a virtual APN named vapn12:
v-apn = vapn12
ACS Timedef Configuration Mode Commands

This configuration mode is only available in StarOS 8.1 and in StarOS 9.0 and later releases.

The ACS Timedef Configuration Mode enables configuring the Time-of-Day Activation/Deactivation feature.

Command Modes

Exec > ACS Configuration > Timedef Configuration

active-charging service service_name > timedef timedef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-timedef) #

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

- end, page 1440
- exit, page 1441
- start, page 1442
end

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

end

**Usage Guidelines**

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 Description**

exit

**Usage Guidelines**

Use this command to return to the parent configuration mode.
**start**

This command allows you to configure timeslots in the current timedef.

---

**Important**

This command is only available in StarOS 8.1 and in StarOS 9.0 and later releases.

**Important**

A maximum of 24 timeslots can be specified within a timedef.

---

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Timedef Configuration

*active-charging service service_name > timedef timedef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-timedef)#
```

**Syntax Description**

- [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

If previously configured, removes the specified timeslot from the current timedef.

- 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

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.
Start time **hh mm ss** end time **hh mm ss**

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 Guidelines**

Use this command to create timeslots in a timedef during which rules have to be active. Timedefs enable activation/deactivation of ruledefs/groups-of-rulledefs such that they are available for rule matching only when they are active.

When a packet is received, and a ruledef/group-of-rulledefs is eligible for rule matching, if a timedef is associated with the ruledef/group-of-rulledefs, 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-rulledefs is considered.

**Important**

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" is after "end time", that rule will span midnight and be considered to be active from the current day until the next day.

If for a timeslot, "start day" is after "end day", that rule will span the current week until 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 without timeslots

**Examples**

The following command specifies a timeslot that starts on **Tuesday** at **09:00:00** and ends on **Friday** at **21:30:00**:

```
start day tuesday time 9 0 0 end day friday time 21 30 0
```

The following command 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 command 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, up to **Tuesday**.

```
start day friday time 22 0 0 end day tuesday time 8 0 0
```
The following command 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 midnight too (that is, 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`
ACS Trigger Action Configuration Mode Commands

The ACS Trigger Action Configuration Mode is used to configure Active Charging Service (ACS) trigger actions.

Command Modes

Exec > ACS Configuration > ACS Trigger Action Configuration

`active-charging service service_name > trigger-action trigger_action_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-trig-action)#
```

Important

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

- charge-request-to-response, page 1446
- end, page 1448
- exit, page 1449
- throttle-suppress, page 1450
- transactional-rule-matching, page 1452
charge-request-to-response

This command allows you to delay charging till the HTTP response for the configured HTTP request method(s).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > ACS Trigger Action Configuration

active-charging service service_name > trigger-action trigger_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-trig-action)#

Syntax Description

| no | charge-request-to-response http { all | connect | delete | get | head | options | post | put | trace } |

no

Disables the response-based charging feature in the trigger-action.

all | connect | delete | get | head | options | post | put | trace

Specifies the HTTP methods applicable to delay charging for a flow.

The Response-based Charging feature supports pipelined HTTP requests (both concatenated and non-concatenated). For pipelined HTTP requests and persistent connections of different HTTP methods, this feature is applied only to those HTTP methods for which it is configured.

- all: Applies to all HTTP methods
- connect: HTTP Connect method
- delete: HTTP Delete method
- get: HTTP Get method
- head: HTTP Head method
- options: HTTP Options method
- post: HTTP Post method
- put: HTTP Put method
- trace: HTTP Trace method
Usage Guidelines
Use this command to delay charging until HTTP response for the configured HTTP request method(s). This CLI command is introduced in support of the Response-based Charging feature. This feature is limited to specified HTTP methods.

**Important**
Response-based charging is supported only for the HTTP protocol.

The Service Scheme configuration is required to configure and enable this feature for a subscriber. For more information on the Response-based TRM feature, see the *ECS Administration Guide*.

Examples
The following command is configured to delay charging for only HTTP Get requests:

```
charge-request-to-response http get
```

The following command is configured to delay charging for HTTP Get and Connect requests:

```
charge-request-to-response http get connect
```
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax Description
end

Usage Guidelines
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 Description
exit

Usage Guidelines
Use this command to return to the parent configuration mode.
throttle-suppress

This command allows you to enable throttle suppression based on trigger condition matched.

Product
- GGSN
- P-GW

Privilege
- Security Administrator
- Administrator

Command Modes
- Exec > ACS Configuration > ACS Trigger Action Configuration
- active-charging service service_name > trigger-action trigger_action_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-trig-action) #

Syntax Description
- \[no\] throttle-suppress

  no
  Disables the Location based QoS Override feature for the subscriber.

  throttle-suppress
  This keyword allows the operators to suppress the throttling when the subscriber is in a particular LAC or TAC location.

Usage Guidelines
Use this command to perform throttle suppression to provide unlimited bandwidth based on the subscriber location. This CLI command is introduced to support Location based QoS Override feature.

To enable this feature for the subscriber, both local-policy and service-scheme framework must be configured. For redundancy support, the corresponding ICSR configuration must also be present.

The service-scheme framework helps in overriding feature behavior specific to a subscriber or a set of subscribers. The user can update the policies specific to subscribers based on pre-configured events. For more information on the service-scheme framework, see the ECS Administration Guide.

Important
This feature requires the license to configure local-policy. For more information on the licensing requirements, contact Cisco account representative.
The previous implementation limits the subscriber bandwidth based on QoS provided by PCRF in order to comply with 3GPP standards. In release 20.2 and beyond, subscriber is provided with unlimited bandwidth by allowing QoS override based on LAC and/or TAC (individual or range) configured in a local-policy (LP) rule on the gateway. If the subscriber is in the LAC or TAC region and hits the LP rule, the gateway ignores the QoS limits imposed by PCRF and allows the subscriber to have unlimited bandwidth.

For more information on this feature, see the *ECS Administration Guide*.

**Examples**

The following command enables throttle suppression for the subscriber:

```
throttle-suppress
```
**transactional-rule-matching**

This command allows you to delay engagement of TRM till the specified HTTP response method(s) for the flow received.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > ACS Trigger Action Configuration

```
active-charging service service_name > trigger-action trigger_action_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-trig-action) #
```

**Syntax Description**

```
no transactional-rule-matching response http { all | connect | delete | get | head | options | post | put | trace }
```

- **no**
  Disables the response-based TRM feature for the subscriber.

- **all | connect | delete | get | head | options | post | put | trace**
  Specifies the HTTP methods applicable to delay engagement of TRM for a flow.

The Response-based TRM feature supports pipelined HTTP requests (both concatenated and non-concatenated). For HTTP requests of different HTTP methods, this feature is applied only to those HTTP methods for which it is configured.

- **all**: Applies to all HTTP methods
- **connect**: HTTP Connect method
- **delete**: HTTP Delete method
- **get**: HTTP Get method
- **head**: HTTP Head method
- **options**: HTTP Options method
- **post**: HTTP Post method
- **put**: HTTP Put method
• **trace**: HTTP Trace method

**Usage Guidelines**

Use this command to delay engagement of TRM till the HTTP response for the configured HTTP request method(s). This CLI command is introduced in support of the Response-based TRM feature. This feature is applicable to all HTTP transactions of a method type for the subscriber, when an HTTP method is configured.

**Important**

Response-based TRM is supported only for the HTTP protocol.

The Service Scheme configuration is required to configure and enable this feature for a subscriber. For more information on the Response-based charging feature, see the *ECS Administration Guide*.

**Examples**

The following command is configured to delay engagement of TRM till HTTP Connect response:

```
transactional-rule-matching response http connect
```
ACS Trigger Condition Configuration Mode Commands

The ACS Trigger Condition Configuration Mode is used to configure Active Charging Service (ACS) trigger conditions.

**Command Modes**

Exec > ACS Configuration > ACS Trigger Condition Configuration

`active-charging service service_name > trigger-condition trigger_condn_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-trig-condn)#
```

**Important**

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

- any-match, page 1456
- end, page 1458
- exit, page 1459
- local-policy-rule, page 1460
- multi-line-or, page 1462
any-match

This command will be applied to analyze all flows created after event activation.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > ACS Configuration > ACS Trigger Condition Configuration

active-charging service service_name > trigger-condition trigger_condn_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-trig-condn)#

Syntax Description

| no | any-match operator condition

no
If previously configured, deletes the specified configuration.

operator
Specifies how to match.

operator must be one of the following:
• !=: Does not equal
• ==: Equals

condition
Specifies the condition to match.
condition must be one of the following:
• FALSE
• TRUE

Usage Guidelines
Use this command to analyze all flows created after event activation.
The following command defines any-match rule to analyze all flows:

```plaintext
any-match = TRUE
```
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

end

Usage Guidelines

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 Description**

`exit`

**Usage Guidelines**

Use this command to return to the parent configuration mode.
local-policy-rule

This command allows you to specify the local-policy rule within ECS for enabling trigger condition.

**Product**
GGSN
P-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > ACS Configuration > ACS Trigger Condition Configuration
active-charging service service_name > trigger-condition trigger_condn_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-trig-condn)#
```

**Syntax Description**

```
[no] local-policy-rule = local_policy_rule
```

- **no**
  - If previously configured, deletes the specified configuration.

- **local-policy-rule**
  - This keyword allows operators to suppress the throttling when the subscriber is in a particular LAC or TAC location and hits the specified local-policy rule. The local-policy-rule contains either a list, range, or index of LAC and/or TAC entries.

  **local_policy_rule**
  - Specifies the local-policy rule name. **local_policy_rule** must be an existing local-policy rule within the service scheme expressed as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to specify the local-policy rule within ECS for enabling trigger condition. This CLI command is introduced in support of the Location based QoS Override feature.

To enable this feature for the subscriber, both local-policy and service-scheme framework must be configured. For redundancy support, the corresponding ICSR configuration must also be present.

The service-scheme framework helps in overriding feature behavior specific to a subscriber or a set of subscribers. The user can update the policies specific to subscribers based on pre-configured events. For more information on the service-scheme framework, see the *ECS Administration Guide*. 
Important  This feature requires the license to configure local-policy. For more information on the licensing requirements, contact Cisco account representative.

Local-policy provides ECS, the list of rules to activate and the list of rules to delete. In case, the rule to be activated is already installed, ECS ignores this rule. Similarly if the rule to be deleted was not installed, ECS ignores this rule as well. The trigger action will be applied only to a subset of traffic that matches the criteria defined under trigger condition.

For more information on this feature, see the *ECS Administration Guide*.

Examples  The following command defines the local-policy rule as zone1.

```
local-policy-rule = zone1
```
multi-line-or

This command allows to check if the OR operator must be applied to all lines in a trigger-condition.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > ACS Trigger Condition Configuration

active-charging service service_name > trigger-condition trigger_condn_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-trig-condn)#

Syntax Description

| no | multi-line-or all-lines

no

If previously configured, deletes the specified configuration.

Usage Guidelines

Use this command to check if the OR operator must be applied to all lines in a trigger-condition.
ACS x-Header Format Configuration Mode

Commands

The ACS 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 Cisco sales representative for more information.

Command Modes

Exec > ACS Configuration > ACS xheader Format Configuration

active-charging service service_name > xheader-format format_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acs-xheader)#

Important

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

- end, page 1464
- exit, page 1465
- insert, page 1466
**end**

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

**Usage Guidelines**
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 Description
exit

Usage Guidelines
Use this command to return to the parent configuration mode.
insert

This command allows you to configure the x-header fields to be inserted in HTTP/WSP GET and POST request packets.

Important

This command is license dependent. Please contact your Cisco accounts representative for more information.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > ACS xheader Format Configuration

active-charging service service_name > xheader-format format_name

Entering the above command sequence results in the following prompt:

{context_name|host_name}(config-acs-xheader)#

Syntax Description

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 | qos | rat-type | s-mcc-mnc | sgsn-address } | acr | congestion-level | customer-id | dest-server-ip-address-port | ggsn-address | mdn | msisdn-no-cc | radius-string | radius-calling-station-id | session-id | sn-rulebase | subscriber-ip-address | time-of-day | username } | encrypt | | http { host | url } | | delete-existing } }
```

no insert xheader_field_name

In StarOS 8.0:

```
insert xheader_field_name { string-constant xheader_field_value | variable { bearer { 3gpp charging-id | ggsn-address | imsi | radius-string | radius-calling-station-id | sgsn-address | sn-rulebase | subscriber-ip-address } | http { host | url } }
```

no

If previously configured, 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 alphanumeric string of 1 through 31 characters.

Up to ten fields can be inserted in each x-header format.
string-constant xheader_field_value
Specifies constant a 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 alphanumeric string of 1 through 63 characters.
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 | qos | rat-type | s-mcc-mnc | sgsn-address } | acr | congestion-level | customer-id | dest-server-ip-address-port | ggsn-address | mdn | msisdn-no-cc | radius-string | radius-calling-station-id | session-id | sn-rulebase | subscriber-ip-address | time-of-day | username } | encrypt }
 bearer { 3gpp { apn | charging-characteristics | charging-id | imei | imsi | qos | rat-type | s-mcc-mnc | sgsn-address } | acr | congestion-level | customer-id | dest-server-ip-address-port | ggsn-address | mdn | msisdn-no-cc | radius-string | radius-calling-station-id | session-id | sn-rulebase | subscriber-ip-address | time-of-day | 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. The APN added via 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.
  • qos: EPC QoS associated with the bearer flow.

The inserted x-header is seen as:
x-bearer-qos: 020400000100000002000000010000000200
• rat-type: This field is deprecated from under bearer rat-type and has been added within bearer 3gpp rat-type. The RAT type as added via bearer 3gpp rat-type.
• s-mcc-mnc: 3GPP serving node MCC + MNC associated with the bearer.

The inserted x-header is seen as: x-s-mcc-mnc: 123765
• sgsn-address: SGSN associated with the bearer flow.

• acr: Anonymous Customer Reference. Only MSISDN part of this is encrypted, if encrypt flag is set.
• congestion-level: Cell level congestion currently experienced by the subscriber.
• customer-id: Customer ID of the bearer.
• dest-server-ip-address-port: The IPv4 or IPv6 address of the Origin Server, and the TCP port of the HTTP request to the Origin Server.
• ggsn-address: GGSN IP address field.
• **imsi**: This field is deprecated from within `bearer imsi` and has been moved within `bearer 3gpp imsi`. The IMSI as added via `bearer 3gpp imsi`.

• **mdn**: MDN of the bearer flow.

• **msisdno-cc**: MSISDN of the mobile handling the flow without the country code.

• **radius-string**: SN-Transparent-Data Attribute received in RADIUS ACCESS ACCEPT message.

• **radius-calling-station-id**: Calling Station ID of the mobile handling the flow. Use this for MSISDN of the mobile handling the flow with the country code.

• **session-id**: Accounting session ID of the bearer flow.

• **sn-rulebase**: Name of the ACS rulebase.

• **sgsn-address**: This field is deprecated from under `bearer sgsn-address` and has been moved within `bearer 3gpp sgsn-address`. The SGSN address as added via `bearer 3gpp sgsn-address`.

• **subscriber-ip-address**: Subscriber IP address.

• **time-of-day**: The current date, time, and time zone offset of the subscriber.

• **username**: User name of the bearer flow.

**encrypt**: Specifies encryption of x-header field configuration. This option must only be configured when x-header encryption is enabled.

```plaintext
http { host | url }
```
Specifies value of the x-header field to be inserted:

- **host**: Host
- **url**: Uniform Resource Locator

**delete-existing**
Specifies enabling detection of spoofing in x-header fields. The x-header field configured with this keyword will be removed from the HTTP header if it already exists, and only the gateway inserted field will remain. By default, anti spoofing is disabled, and if required, should be enabled at a field level.

**Usage Guidelines**
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 the 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.

**Examples**
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:

```plaintext
insert test12 string-constant testing
```
ALCAP Configuration Mode Commands

Important
In Release 20.0, HNBGW is not supported. Commands in this configuration mode must not be used in Release 20.0. For more information, contact your Cisco account representative.

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.

Command Modes

Exec > Global Configuration > Context Configuration > ALCAP Service Configuration

configure > context context_name > alcap-service service_name

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-alcap-service-service_name)#

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

- aal2-node, page 1470
- aal2-route, page 1472
- associate, page 1474
- end, page 1475
- exit, page 1476
- maximum reset-retransmission, page 1477
- self-point-code, page 1478
- timeout alcap, page 1480
- timeout stc, page 1483
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

**Command Modes**

Exec > Global Configuration > Context Configuration > ALCAP Service Configuration

`configure > context context_name > aalcap-service service_name`

Entering the above command sequence results in the following prompt:

`{context_name}host_name(config-alcap-service-service_name)#`

**Syntax Description**

`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 Guidelines**

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}host_name(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*.

Examples

Following command creates AAL2 node configuration mode named `aal2_1` within the specific ALCAP service for \[\text{IuCS-over-ATM support towards CS core networks and switch the user to AAL2 Node Configuration Mode named `aal2_1`:}
\]

```
  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

Command Modes
Exec > Global Configuration > Context Configuration > ALCAP Service Configuration
configure > context context_name > alcap-service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-alcap-service-service_name)#

Syntax Description

**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.

**aal2-node aal2_node_name**

Identifies the name of the AAL2 node name to configure in AAL2 route.

The **aal2_node_name** must be an alphanumerical string from 1 through 63 characters.

Usage Guidelines
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.

---

**Examples**  Following command create a mapping between ATM endpoint MGW1 and AAL2 node aal2_1 for AAL2 connection routing purposes:

```
> 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

Command Modes

Exec > Global Configuration > Context Configuration > ALCAP Service Configuration

class > context context_name > a1cap-service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-alcap-service-service_name) #

Syntax Description

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 LuCS-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 Guidelines

Use this command to associate a pre-configured SS7 routing domain index to provide LuCS-over-ATM support towards CS core network for HNB subscriber.

A maximum of TBD SS7 routing domains can be configured in one ALCAP service.

Examples

Following command associates a predefined SS7 routing domain id 3 with ALCAP service to define routing domain for LuCS-over-ATM supprot 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 Description**

end

**Usage Guidelines**

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 Description
exit

Usage Guidelines
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

**Command Modes**

Exec > Global Configuration > Context Configuration > ALCAP Service Configuration

`configure > context context_name > alcap-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-alcap-service-service_name)#
```

**Syntax Description**

`maximum reset-retransmissions retries`

`default maximum reset-retransmissions`

`default`

Sets the number of RESET message retries to default value of 1.

`retries`

Sets the maximum number of retries allowed for transmission of RESET message to reset the AAL2 path by ALCAP service.

`retries` must be an integer value from 0 through 4. When 0 is used retransmission will be disabled.

Default: 1

**Usage Guidelines**

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.

**Examples**

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

**Command Modes**

Exec > Global Configuration > Context Configuration > ALCAP Service Configuration
configure > context context_name > aalcap-service service_name

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-alcap-service-service_name)#

**Syntax Description**

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.

point_code: 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 Guidelines**

Use this command to assign the self point code to use for this ALCAP service.

**Examples**

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

**Command Modes**
Exec > Global Configuration > Context Configuration > ALCAP Service Configuration

```
configure > context context_name > alcap-service service_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-alcap-service-service_name)#
```

**Syntax Description**

```
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.

`blo_TIMER_VALUE` must be an integer value from 2 through 60.

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 esblish 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.

\textit{erq\_timer\_value} must be an integer value from 5 through 30.

Default: 5

\textbf{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 \textbf{Timer\_MOD} timer. The timer waits for specified timeout duration \textit{mod\_timer\_value} for ALCAP-MODIFY-CONFIRM message before reporting error in procedure and system requests ALCAP Manager to initiate 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.

\textit{mod\_timer\_value} must be an integer value from 5 through 30.

Default: 5

\textbf{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 \textbf{Timer\_REL} timer and sends RAB-ASST-REQ to HNB. The timer waits for specified timeout duration \textit{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.

\textit{rel\_timer\_value} must be an integer value from 2 through 60.

Default: 2

\textbf{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 \textbf{Timer\_RES} timer. The timer waits for specified timeout duration \textit{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.

\textit{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 starts 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 Guidelines

Use this command to configure the timeout duration for various ALCAP procedures in ALCAP service.

Examples

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 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

Command Modes

Exec > Global Configuration > Context Configuration > ALCAP Service Configuration

configure > context context_name > aalcap-service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-alcap-service-service_name)#

Syntax Description

timeout stc {long long_timer_value | short short_timer_value}

default 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 Guidelines**

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.

**Examples**

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
```
APN Profile Configuration Mode

Essentially, an APN profile is a template that consists of a set of APN-specific commands that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the set of commands in the associated APN profile will be applied. The same APN profile can be associated with multiple APNs and multiple operator policies.

The SGSN and the MME each support a total of 1,000 APN profile configurations per SGSN/MME; up to 50 APN profiles can be associated with a single operator policy. For additional SGSN limit information, refer to Engineering Rules in the SGSN Administration Guide.

The APN Profile configuration mode defines a set of parameters controlling the SGSN or MME behavior when a specific APN is received or no APN is received in a Request. An APN profile is a key element in the Operator Policy feature and an APN profile is not used or valid unless it is associated with an APN and this association is specified in an operator policy (see the Operator Policy Configuration Mode Commands).

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Important**

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

- accounting context, page 1488
- accounting mode, page 1489
- active-charging rulebase, page 1490
- address-resolution-mode, page 1492
- apn-resolve-dns-query, page 1494
- apn-restoration, page 1495
- apn-type, page 1497
• qos apn-ambr, page 1552
• qos class, page 1553
• qos dedicated-bearer, page 1560
• qos default-bearer, page 1561
• qos pgw-upgrade, page 1563
• qos prefer-as-cap, page 1565
• qos rate-limit direction, page 1567
• ranap allocation-retention-priority-ie, page 1572
• restrict access-type, page 1575
• sm t3396, page 1577
• timeout bearer-inactivity, page 1579
• timeout idle, page 1581
• twan, page 1583
• virtual-mac, page 1584
accounting context

This command allows you to define the name of the accounting context and associate a GTPP group with this APN profile.

Product
SaMOG

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax Description

accounting context context_name gtpp group group_name
remove accounting context

remove
Removes the accounting configuration from this profile's configuration.

context_name
Specifies the accounting context. context_name must be an alphanumeric string of 1 through 79 characters.

gtpp group group_name
Identifies the GTPP group, where the GTPP related parameters have been configured in the GTPP Group Configuration mode, to associate with this SaMOG APN profile.

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

Usage Guidelines
Use this command to associate a predefined GTPP server group, including all its associated configuration, with a specific SaMOG APN profile. Even if an accounting context is also specified in a call control profile, the priority is given to the accounting context of the APN profile.

Examples
The following command identifies an accounting context called account1 and associates a GTPP server group named roaming with defined charging gateway accounting functionality:

accounting context account1 gtpp group roaming
**accounting mode**

This command allows you to define the mode of accounting to be performed for this SaMOG APN profile.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local] host_name{apn-profile-profile_name}#

**Syntax Description**
accounting mode { gtp | none }
{ default | remove } accounting mode

- **default**
  Resets the accounting mode to GTPP.

- **remove**
  Removes the accounting mode from this profile's configuration.

- **gtp**
  Specifies that GTPP accounting is performed. This is the default method.

- **none**
  Specifies that no accounting will be performed for the APN profile.

**Usage Guidelines**
Use this command to specify the accounting mode for an SaMOG APN profile to generate bearer-based SaMOG CDRs. Even if an accounting mode is also specified in a call control profile, the priority is given to the accounting mode of the APN profile.

**Examples**
The following command specifies that no accounting will be used for the APN profile:

accounting mode none
active-charging rulebase

Configure the name of the rulebase that contains the charging action for the HTTP redirection and the URL for the portal for SaMOG web authorization, and/or the rulebase that contains the NAT policy for the SaMOG Local Breakout feature.

**Product**  
SaMOG

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > APN Profile Configuration  
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:  
[local] host_name(apn-profile-profile_name)#

**Syntax Description**  
active-charging rulebase rulebase_name  
no active-charging rulebase

no  
If previously configured, removes the ACS rulebase to be used.

rulebase rulebase_name  
Specifies the active charging rulebase to be used.

rulebase_name must be the name of an ACS rulebase, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters.

**Usage Guidelines**  
Use this command to configure the name of the rulebase that contains the charging action for the HTTP redirection and the URL for the authentication portal to facilitate HTTP redirection to the authorization portal during the pre-authentication phase, and/or the rulebase that contains the NAT policy for the SaMOG Local Breakout feature. The ACS rulebase specified in this configuration will be used only if the AAA server does not specify the ACS rulebase during the pre-authentication phase.

**Important**  
This command is license dependent. Contact your Cisco account representative for more information on SaMOG feature license requirements.
The following command configures the rulebase `webauthredir`:

```
active-charging rulebase webauthredir
```
address-resolution-mode

Identifies the address resolution mode for this APN profile.

---

**Important**

From release 16.2 onwards, the S4-SGSN also supports this command.

---

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name (apn-profile-profile_name)#
```

**Syntax Description**

address-resolution-mode { fallback-for-dns | local }

default address-resolution-mode

default

Resets the configuration to the default value, that is, **fallback-for-dns**.

**fallback-for-dns**

Instructs the system to try DNS resolution. If the DNS query fails, the SGSN will use locally configured addresses, if they have been configured. The pgw-address configured under apn-profile will be treated as fallback for dns address and will used only after dns failure.

Default: enabled

---

**Important**

This address will be used on DNS SNAPTR Failure except on Service parameter mismatch.

If pgw-address-resolution-mode fallback-for-dns is not configured then the gateway-address will be treated as fallback for DNS address and UE will fallback to Gn-SGSN, if GPRS-Subscription is available.

**local**

Instructs the system to only use locally configured addresses and not to use DNS query.
Default: disabled

**Usage Guidelines**  
Use this command to specify the DNS query or local address resolution for this APN profile.

**Examples**  
The following command sets the address resolution mode to use local addresses *only if* the DNS query fails:  
`address-resolution-mode fallback-for-dns`
apn-resolve-dns-query

Command enables the SGSN to send Straightforward Name Authority Pointer (SNAPTR) type DNS query for APN resolution on a per APN basis.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (apn-profile-profile_name) #
```

**Syntax Description**
```
apn-resolve-dns-query snaptr [epc-ue | non-epc-ue] remove apn-resolve-dns-query snaptr
```

- **remove**
  Removes the DNS SNAPTR function from the configuration.

- **epc-ue**
  Configures the S-NAPTR queries to be applicable for EPC-capable UE.

- **non-epc-ue**
  Configures the S-NAPTR queries to be applicable for non-EPC-capable UE.

**Usage Guidelines**
SNAPTR filters based on the EPC-capability of the user equipment (UE). Use this command to enable SNAPTR type DNS query for APN resolution for 3G subscribers with EPC subscription. Configuration in this mode promotes control of this feature per APN.

If neither of the keywords is included with the configuration, then S-NAPTR query is applicable to all UE, both EPC-capable UE and non-EPC capable UE.

By default, this functionality is not enabled.

**Examples**
Enable the SGSN to select a PGW during APN resolution:

```
apn-resolve-dns-query snaptr
```
apn-restoration

Configures the APN restoration priority value.

**Product**
- MME
- SGSN

**Privilege**
- Security Administrator
- Administrator

**Command Modes**
- Exec > Global Configuration > APN Profile Configuration
- configure > apn-profile *profile_name*

Entering the above command sequence results in the following prompt:
```
[local]{host_name}{apn-profile-*profile_name}#
```

**Syntax Description**
- `apn-restoration priority *priority_value*`
- `remove apn-restoration priority`

- **remove**
  Removes the APN restoration priority value from the configuration.

- **priority *priority_value***
  Configures the APN restoration priority value. The reactivation of PDNs after a P-GW restart notification is processed in the order of this priority.

- **priority_value**
  The priority value is an integer value from 1 through 16. Where "1" is the highest priority and "16" is the lowest priority. Default: 16 (lowest priority).

**Usage Guidelines**

The PGW Restart Notification (PRN) message is sent by the S-GW when it detects a peer P-GW has restarted. After the affected subscribers have been deactivated, the MME/S4-SGSN will prioritize the re-activation of impacted PDN connections based on subscribed APN restoration priority, if received from the HSS. If an APN restoration priority is not received from the HSS, then this locally configured value is used. If there is no local configuration then by default such PDNs will be assigned the lowest restoration priority.

- The MME will only restore PDNs for which the APN restoration priority is configured and/or received from HSS. Otherwise PDNs will be released by regular deactivation.
For the MME, refer to the LTE Policy > LTE Emergency Profile > **apn** command to define a different APN restoration priority for emergency sessions for this APN profile.

**Examples**

The following command is used to configure the APN restoration priority value of "10" for an APN profile:

```
apn-restoration priority 10
```
apn-type

Identifies the type of APN as an IMS APN.

**Product**

- ePDG
- SGSN
- MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax Description**

```
apn-type { emergency | ims } [ pcsf-restoration { pco-update | pdn-deactivate } ]
remove apn-type ims
```

**remove**

Erases this identification configuration from the APN profile and resets the APN profile to the default behavior which disables the APN type as IMS.

**emergency**

Identifies the APN as EMERGENCY APN.

**ims**

Identifies the APN as IMS APN. If an IMS APN is present, Modify Bearer Req/Update PDP Req will be delayed during Inbound SRNS relocation for SGSN.

**pcsf-restoration { pco-update | pdn-deactivate }**

- **pcsf-restoration**: The pcsf-restoration keyword in this command identifies P-CSCF restoration for IMS PDN. This keyword is functional only if the feature license is installed.
- **pco-update**: The pco-update keyword selects P-CSCF restoration method as PDN Modification through PCO update.
**pdn-deactivate**: The pdn-deactivate keyword selects P-CSCF restoration method as PDN Deactivation. This is the default method.

---

**Important**

If only "apn-type ims" is configured, then the default P-CSCF restoration method **pdn-deactivate** is enabled.

---

**Usage Guidelines**

This command identifies the APN as an IMS APN. This enables the SGSN to delay sending Modify Bearer Request to the S-GW until after receiving the Forward Relocation Complete Ack from the peer during SRNS procedure.

Also, the following CLI identifies an APN as IMS APN and to configure to indicate whether the PGW supports optional extension or if the MME initiates PDN deactivation for HSS initiated P-CSCF restoration. To enable HSS-based P-CSCF Restoration, use the pcsf-restoration command under the Call Control Profile mode.

**Examples**

Identify the APN for this profile as an IMS type APN:

```
apn-type ims
```

The following command selects pco-update as the P-CSCF Restoration method:

```
apn-type ims pcsf-restoration pco-update
```

The following command selects pdn-deactivate as the P-CSCF Restoration method:

```
apn-type ims pcsf-restoration pdn-deactivate
```
associate accounting-policy

Associates the APN with specific pre-configured policies configured in the same context for SaMOG charging.

**Product**
SaMOG

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (apn-profile-profile_name)#
```

**Syntax Description**

```
associate accounting-policy policy_name
remove associate accounting-policy
```

- **remove**
  Removes the association of the policy from the APN profile.

  **policy_name**
  Specified the policy name to associate to the APN profile. `policy_name` must be an existing accounting policy, and must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to associate the SaMOG APN profile with an accounting policy configured in this context to provide triggers to generate CDRs. The accounting policy configured under the APN profile takes priority over the accounting policy configured under the call control profile.

**Examples**

The following command associates this SaMOG APN with an accounting policy called `acct1`:

```
associate accounting-policy acct1
```
associate qci-qos-mapping

Provides operators with a configuration to associate a Qos Class Identifier (QCI) Quality of Service (QoS) mapping table with a specified APN profile configuration.

**Product**
- SGW
- SAE-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > APN Profile Configuration
- configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

```
[local] host_name (apn-profile-profile_name) #
```

**Syntax Description**

```
[ remove ] associate qci-qos-mapping mapping_table_name
```

- `remove`
  Removes the specified QCI to QoS mapping table association.

- `associate qci-qos-mapping mapping_table_name`
  Instructs the application to associate the specified QCI QoS mapping to this APN profile.

**Usage Guidelines**
Associates a QCI QoS mapping table with an APN profile.

**Examples**
This example associates a QCI QoS mapping table with the APN Profile 'QCIQOSMap'.

```
associate qci-qos-mapping QCIQOSMap
```
associate quality-of-service-profile

Associates the specified Quality of Service profile with the APN profile.

Product
- MME
- SGSN

Privilege
Administrator

Command Modes
- Exec > Global Configuration > APN Profile Configuration
- configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local] host_name(apn-profile-profile_name)#

Syntax Description
- associate quality-of-service-profile qos_profile_name access-type [ eps | gprs | umts ]
- remove associate quality-of-service-profile access-type [ eps | gprs | umts ]

- remove
Removes the association of the specified Quality of Service profile with the APN profile.

- access-type
Configures the access-types to be associated with the QoS profile for this APN profile.

  - eps identifies a 4G EPS network. (MME only)
  - gprs identifies a 2G GPRS network.
  - umts identifies a 3G UMTS network.

- qos_profile_name
Identifies the name of the Quality of Service profile to be associated with the APN profile.

Usage Guidelines
This command identifies a specific Quality of Service profile to be associated with the APN profile.

Examples
Use this command to associate a 3G (UMTS) QoS profile named test with the APN profile.

associate quality-of-service-profile test access-type umts
Use this command to associate a 4G QoS profile named MMEqos1 with the APN profile.

```
associate quality-of-service-profile MMEqos1 access-type eps
```
associate sgw-paging-profile

This command allows the association of an SGW Paging Profile with an APN profile on the S-GW.

Product
S-GW

Privilege
Administrator, Security Administrator

Command Modes
Exec > Global Configuration > APN Profile Configuration
   configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:
   [local] host_name(apn-profile-profile_name)#

Syntax Description
   [ remove ] associate sgw-paging-profile three-tupple

   remove
   Removes the S-GW Paging Profile from the APN Profile.

   associate sgw-paging-profile three-tupple
   Associates an SGW Paging Profile with an APN profile on the S-GW. S-GW Paging Profiles are configured in Global Configuration Mode with the sgw-paging-profile three-tupple command.

Usage Guidelines
Use this command to associate an S-GW paging profile with an APN profile on the S-GW.

Examples
This example associates an S-GW paging profile with an APN profile on the S-GW.
   associate sgw-paging-profile three-tupple
CC

Configures the charging characteristics (CC) for this APN profile.

Product

SGSN
S-GW
SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax Description

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 from this APN profile.

local-value-for-scdrs behavior bit_value profile index_bit

Sets the value of the behavior bits and profile index for the charging characteristics for S-CDRs locally, when the Home Location Register (HLR) does not provide these values.

If the HLR provides the charging characteristics with behavior bits and profile index, and the operator wants to ignore what the HLR provides, then specify the 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 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
• 8 for normal billing
Defaults: $bit_value = 0x0$; $index_bit = 8$

prefer { hlr-value-for-scdrs | local-value-for-scdrs }

Specify what charging characteristic settings the system will use for S-CDRs.

- **hlr-value-for-scdrs**: instructs the system to use charging characteristic settings received from the HLR for S-CDRs.

- **local-value-for-scdrs**: instructs the profile preference to only use locally configured/stored charging characteristic settings for S-CDRs.

Default: **hlr-value-for-scdrs**

**Usage Guidelines**

Use this command to specify the charging characteristic for S-CDRs -- either from the HLR or locally from the SGSN.

These charging characteristics parameters for S-CDRs and M-CDRs are also configurable in the Call-Control Profile configuration mode. When CC parameters are specified in both types of profiles, then:

- For generation of M-CDRs, the parameters configured in the Call-Control Profile configuration mode will take precedence.

- For generation of S-CDRs, the parameters configured in the APN Profile configuration mode will take precedence.

**Examples**

The following command configures the APN profile to instruct the SGSN not to use charging characteristic settings received from the HLR for S-CDR generation:

```
cc prefer hlr-value-for-scdrs
```
**dedicated-bearers**

Configures the MME to either accept or reject dedicated GBR and Non-GBR bearers.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local] host_name (apn-profile-profile_name) #

**Syntax Description**

`dedicated-bearers { gbr { accept | reject } | non-gbr { accept | reject } }`

`| remove | dedicated-bearers { gbr | non-gbr }`

**remove**

Removes the configuration, returning the system to the default setting where the MME accepts GBR or Non-GBR dedicated bearers.

`gbr { accept | reject }

Configures the MME to accept or reject dedicated GBR bearers.

`non-gbr { accept | reject }

Configures the MME to accept or reject dedicated Non-GBR bearers.

**Usage Guidelines**

The MME differentiates GBR and Non-GBR dedicated bearers as follows: GBR Bearers - QCI value ranges from 1 to 4; Non-GBR bearers - QCI value ranges from 5-9.

In the case of a UE-initiated Bearer Resource Allocation Reject, the ESM cause "EPS QOS not accepted" is used and the corresponding bearer allocation reject MME statistic is incremented.

In the case of a Create Bearer Request Reject, the EGTP cause "Service denied" is used and the corresponding EGTP statistic is incremented.

Note: Handling of multiple bearers in a Create Bearer request from S-GW for Partial accept/reject of GBR/Non-GBR dedicated bearers is a current limitation.
Examples

The following commands configure the MME to reject both GBR and Non-GBR dedicated bearers:

- `dedicated-bearers gbr reject`
- `dedicated-bearers non-gbr reject`
**description**

Defines a descriptive string relevant to the specific APN profile.

**Product**

- MME
- SGSN
- S-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

- Exec > Global Configuration > APN Profile Configuration
- `configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax Description**

- `description description`
- `remove description`

**remove**

Removes the configured description from this APN profile.

**description**

Specifies a description for this APN profile as an alphanumeric string of 1 through 100 characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotation marks (").

**Usage Guidelines**

Define information that identifies this particular APN profile.

**Examples**

Indicate that APN profile *apnprof1* is to be used for customers in Saudi Arabia and that the profile was created on April 10th of 2010:

```
description "apnprof1 defines APNs for customers in Saudi Arabia (4/10/10)."
```
dhcp lease

Configures a lease period for the UE's IP address during SaMOG Web Authorization pre-authentication and TAL phases.

**Important**

This command requires the SaMOG Web Authorization feature license. For more information, contact your Cisco account representative.

**Product**

SaMOG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

```bash
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```bash
[local]host_name(apn-profile-profile_name)#
```

**Syntax Description**

```
dhcp lease { short duration | time duration }
default dhcp lease { short | time }
remove dhcp lease short
```

**default**

Restores the DHCP lease configuration for short lease time (pre-authentication phase) and DHCP lease time (TAL phae) to its default value.

**remove**

If previously configured, removes the DHCP short lease time configuration from this APN profile.

**short duration**

Specifies the DHCP short lease time for web authorization sessions to force the UE to initiate DHCP request after the pre-authentication phase completes.

*duration* must be an integer from 2 through 600.

Default: 20 seconds
time duration

Specifies the lease time for the UE's IP address during the web authorization TAL phase.

duration must be an integer from 600 through 4294967295.

Default: 4294967295 seconds

Usage Guidelines

Use this command to configure a lease period for the UE's IP address during SaMOG Web Authorization pre-authentication and TAL phases.

Examples

The following command configures a DHCP short lease period of 60 seconds and lease period of 3600 seconds:

```
dhcp lease short 60 time 3600
```
direct-tunnel

Defines the permission for direct tunnel establishment by GGSNs. This command is specific to the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local] host_name{apn-profile-profile_name}#

Syntax Description

direct-tunnel not-permitted-by-ggsn
remove direct-tunnel

remove

Removes the direct tunnel establishment configuration from this APN profile.

not-permitted-by-ggsn

Specifies that a direct tunnel is not permitted by the GGSN when resolved by this APN.
Default: disabled.

Usage Guidelines

Use this command to enable/disable the permission for establishment of direct tunnels between an RNC and a GGSN.

Examples

The following command instructs the SGSN not to permit establishment of a direct tunnel with a GGSN:
direct-tunnel not-permitted-by-ggsn
**dns**

Configure the primary and secondary IPv4 or IPv6 address of the DNS servers.

**Product**
SaMOG

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

```text
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```text
[local] host_name (apn-profile-profile_name) #
```

**Syntax Description**

```text
dns [ipv6] {primary | secondary} ip_address
| no | dns | ipv6 | {primary | secondary}
```

- **no**
  If previously configured, removes the DNS primary or secondary IP address to be used for web authorization.

- **ipv6**
  Specify IPv6 DNS server(s) to enable Flow-based Local Breakout GTPv2 sessions.

- **primary | secondary IP_address**
  Specify the primary or secondary DNS server address using the **primary | secondary** keywords.

  *ip_address* must be expressed in IPv4 dotted-decimal or IPv6 colon-separated (when the **ipv6** keyword is configured) notation format.

**Usage Guidelines**

Use this command to configure the IPv4 or IPv6 address of the primary and secondary DNS servers to be used during session setup. The primary and secondary DNS servers specified in this configuration will be used only if the AAA server does not specify the same.

**Important**

This command is license dependent. Contact your Cisco account representative for more information on SaMOG feature license requirements.
The following command configures a primary DNS server with the IP address 162.123.23.1:

dns primary 162.123.23.1
**dns-extn**

Takes an offset group of digits from the MSISDN and appends the digits to the DNS query string to create a new APN intended to assist roaming subscribers to use the local GGSN.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]<host_name>(apn-profile-profile_name)#
```

**Syntax Description**

```
dns-extn { charg-id { binary | decimal | hexadecimal } | lac-rac | msisdn start-offset start_digits end-offset end-digits | rnc-id [ charg-id { binary | decimal | hexadecimal } ] }  
remove dns-extn { charg-id | lac-rac | msisdn | rnc-id | charg-id }  
```

- **charg-id** { binary | decimal | hexadecimal }
  
  Instructs the SGSN to take the profile index value of the charging characteristics, from the PDP subscription record (selected during APN selection) and include the profile index value in the APN name prior to sending out DNS queries. The operator can also specify the format (binary, decimal or hexadecimal) for the CC information to be included.

- **lac-rac**

  Enables the SGSN to append geographical information to the APN string that is being sent in the DNS query. This information is used during the DNS query process to select the geographically closest GGSN.

- **msisdn start-offset start_digits end-offset end-digits**

  Defines an offset group of digits from the MSISDN and appends the digits to create a new APN DNS query string that is intended to assist roaming subscribers to use the local GGSN.

  - **start_digits** is an integer from 1 through 14 that identifies the position of the first digit in the MSISDN to start the offset.
  
  - **end-digits** is an integer from 2 through 15 that identifies the position of the last digit in the MSISDN to be part of the offset.
rnc-id { charg-id { binary | decimal | hexadecimal } }

Instructs the SGSN to include the ID of the calling RNC in the APN DNS query string. Optionally, the profile index value of the charging characteristics can be inserted into the APN name prior to sending out DNS queries. As well, the operator can specify the format (binary, decimal or hexadecimal) for the CC information to be included.

Usage Guidelines

With this command, the APN in the DNS query string, used for querying the GGSN address, can be appended with additional information, such as

- digits from the MSISDN
- LAC/RAC info
- RNC-ID
- profile index from the charging characteristics information (SCHAR)

This additional information allows some customization of the DNS query string to facilitate selecting a specific (usually local or nearest) GGSN.

For example, roaming subscribers using a specific APN may want to be directed to a specific GGSN. This can be achieved by having an operator policy for roaming subscribers associated with an APN profile that includes a configuration specifying certain digits, from the MSISDN or geographical information from the LAC/RAC, be appended to the APN. This is then used as the DNS query string.

In addition, the operator must configure appropriate DNS entries to enforce the selection of the required GGSN. After appending the MSISDN digits to the DNS query string, the string will have the form:

\[ \text{ni.<digits>}.mnc*.mcc*.gprs \]

After appending the LAC/RAC information to the DNS query string, the string will have the form:

\[ <\text{apn_network_id}>.racAAAA.lacBBBB.<\text{apn_operator_id}> \]

where the AAAA and BBBB are Hex-coded digits (less than 4 significant digits and one or more zero ("0") digits will be inserted to the left side of the Hex to fill the 4-digit coding).

After appending the charging characteristic (SCHAR) information, the DNS string will take the following form:

\[ <\text{apn_network_id}>.<\text{profile_index}>.<\text{apn_operator_id}> \]

The profile index in the following example has an integer value 10:

\[ \text{quicknet.com.uk.1010.mnc234.mcc027.gprs} \]

If the RNC-ID information is configured to be a part of the APN name, and if inclusion of the profile index of the charging characteristics information is also enabled before the DNS query is sent, the profile index is included after the included RNC-ID and the DNS APN name will appear in the following form:

\[ <\text{apn_network_id}>.<\text{rnc_id}>.<\text{profile_index}>.<\text{apn_operator_id}> \]

Once the DNS extension is defined, the selected extension is applicable when either the wildcard APN feature or the default APN feature are configured and used.

The information is appended to the DNS query and the actual APN string sent to the GGSN will not be modified in any way.
**Examples**

A sample MSISDN is '11223344566778' and a sample APN NI (network identifier) is 'wap98.testnetz.ca'. The following command instructs the SGSN to create a new APN with digits pulled from the MSISDN and appended to the APN:

```
msisdn start-offset 3 end-offset 9
```

The resulting APN DNS query string would have appended 7 digits (2233445) to the APN NI so that it would appear something like wap98.testnetz.ca.2233445.MNC009.MCC262.GPRS

Enable inclusion of geographical information in the APN string used for the DNS query to locate the closest GGSN:

```
lac-rac
```

In the following example, the DNS query for a subscriber using RNC 0321 with the profile index of value 8 would appear as:

```
quicknet.com.uk.0321.1000.mnc234.mcc027.gprs
```
end

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

`end`

**Usage Guidelines**

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 Description
exit

Usage Guidelines
Use this command to return to the parent configuration mode.
gateway-address

Configures the IPv4 or IPv6 address of the GGSN supporting the APN associated with this APN profile. Also, use this command to create a secondary pool of GGSNs. This command is specific to the SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration  
configure > apn-profile profile_name  
Entering the above command sequence results in the following prompt:  
[local] host_name{apn-profile-profile_name}#

**Syntax Description**
\[gateway-address \ ip_address \ {priority priority | weight weight | secondary-pool \} \]
\[no gateway-address \ ip_address\]

**no**
Disables the GGSN address configured in this APN profile.

\[ip_address\]
Specifies the IP address for the GGSN in IPv4 dotted-decimal or IPv6 colon-separated notation.

\[priority priority\]
Specifies the priority, for the configured GGSN address, to be considered during address selection. If the highest priority GGSN fails to respond, the next priority level GGSN is selected. priority is an integer from 1 through 100. Note that the lower integer has the higher priority, so that 1 is the highest priority.

\[weight weight | secondary-pool\]
Specifies the weight (preference) assigned to a GGSN to facilitate load balancing. weight is an integer from 1 to 100 where 1 is the least preferred and 100 is the most preferred.

If a weight is assigned to an address, 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 that the sum of the weights does not need to be 100. The calculation of weight
percentiles is carried out proportionately, 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

secondary-pool
This optional keyword allows the operator to enable multiple GGSN pools by assigning the GGSN to a secondary pool of GGSNs. The selection algorithm for GGSNs in a secondary pool is weight-based.

Usage Guidelines
Use this command to define priority or load balancing to be applied during GGSN selection. A maximum of 16 GGSN address can be configured for this APN profile.

Also use this command to setup GGSN pools - primary and secondary pools with up to 16 GGSNs in each pool. By default, GGSNs will always be selected from the primary pool. However, working in tandem with the ggsn-fail-retry-timer command configuration (SGTP service configuration mode) which enables the local DNS feature, some of the primary GGSNs can be temporarily blacklisted if they become unavailable or overburdened.

Examples
Set a GGSN address with a secondary priority level:
\texttt{gateway-address 123.123.123.2 priority 2}

Add a GGSN to the secondary GGSN pool and define selection weighting of 7th:
\texttt{gateway-address 198.168.138.8 weight 7 secondary-pool}
**gateway-selection**

Configures gateway selection related parameters for ePDG and SaMOG.

**Product**
- ePDG
- SaMOG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

**Syntax Description**

For ePDG,

```
gateway-selection alternate-epdg strip-labels strip_labels max-alternate-pgw max_alternate_pgw_attempts
```

```
remove gateway-selection alternate-epdg strip-labels strip_labels max-alternate-pgw
```

For SaMOG,

```
gateway-selection max-alternate-pgw max_alternate_pgw_attempts
```

```
remove gateway-selection max-alternate-pgw
```

remove

If previously configured, disables the maximum number of P-GW address resolution for this APN profile.

**alternate-epdg**

---

**Important**
This keyword is license dependent. Contact your Cisco account representative for more information on ePDG feature license requirements.

(ePDG) Enables alternate ePDG selection.
strip-labels strip_labels

**Important**
This keyword is license dependent. Contact your Cisco account representative for more information on ePDG feature license requirements.

(ePDG) Number of labels to be stripped off for domain matching.

*strip_labels* must be an integer between 0 to 10 separated by periods. Default value is 3.

**max-alternate-pgw max_alternate_pgw_attempts**

(ePDG/SaMOG) Configures maximum number of alternate P-GW attempts.

*max_alternate_pgw_attempts* must be an integer between 0 to 64.

**Usage Guidelines**
Use this command to configure the gateway selection related parameters.

For ePDG, use this command to configure the maximum number of labels to be stripped off for domain matching, and the maximum number of alternate P-GW attempts.

For SaMOG, use this command to configure the maximum number of alternate P-GW attempts during P-GW selection fall-back.

**Examples**
The following example to set the maximum alternate P-GW selection attempts to 8:

gateway-selection max-alternate-pgw 8
**gn-gtp-version**

This command enables the operator to prevent the SGSN from attempting GTPv0 Requests for GGSNs associated with specified APNs so that the SGSN tries activation with the next available GGSN if the current GGSN does not respond after the GTPv1 Request retries fail.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

`configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(apn-profile-profile_name) #
```

**Syntax Description**

`[ remove ] gn-gtp-version v1-only`

- **remove**
  
  Used with the command, this filter erases the previous GTPv1 configuration and returns the SGSN configuration to the default value of both GTPv1 and GTPv0.

- **v1-only**
  
  This extension must be included to complete the command. This extension disables GTPv0 fallback.

**Usage Guidelines**

During activation, the SGSN sends GTPv1 PDP Requests a GGSN and if no response is available from the GGSN after the maximum number of retransmissions and timeout, then before trying an alternate GGSN, the SGSN attempts to create GTPv0 PDP Requests and retries are carried out. Only after GTPv0 retransmissions and timeout would the SGSN try activation with the next available GGSN.

The SGSN supported GTPv0 fallback. After exhausting all configured retry attempts for GTPv1, the SGSN would retry the GTP-C Request using GTPv0. This fallback is conditional and is done only when the GTP version of a GGSN is unknown during the first attempt at activating a PDP context with the GGSN.

This command allows the operator to disable the GTPv0 fallback for GTP-C Requests to GGSNs corresponding to a specific APN, thus reducing unnecessary signalling if all known GGSN support GTPv1 only. Hence, if more than one GGSN address is returned by the DNS server during activation, then the SGSN more immediately attempts activation with the next GGSN after exhausting all the GTPv1 retry attempts. If only one GGSN address is returned, then the SGSN rejects the activation after exhausting all the configured GTPv1 retries.
Examples

The following command disables GTPv0 fallback:

```
gn-gtp-version v1-only
```

The following command deletes the previous configuration and re-enables the default so the SGSN will attempt activation via both GTPv1 and if needed GTPv0:

```
remove gn-gtp-version v1-only
```
**gtp**

Enables or disables the GTPC private extension for the Overcharging Protection feature. This command is specific to the SGSN.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

```
[local] host_name(apn-profile-profile_name)#
```

**Syntax Description**

```
| remove | gtp private-extension loss-of-radio-coverage send-to-ggsn | send-to-peer-sgsn |
```

**remove**

Disables the inclusion of the GTPC private extension, thereby disabling the Overcharging Protection feature.

**private-extension loss-of-radio-coverage send-to-ggsn**

Instructs 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 extensions are only understood by a GGSN with an Overcharging Protection license.

The mandatory **loss-of-radio-coverage send-to-ggsn** keyword set instructs the SGSN to forward the private extension flag to the GGSN in the event of a 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 Guidelines**

**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 to 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, 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 Administration Guide* for additional information regarding the Overcharging Protection feature.

**Examples**

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
```
idle-mode-acl

Configures a group of access control lists (ACLs) that define rules to apply to downlink data destined for UEs in an idle mode.

**Product**

S-GW
SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

**Syntax Description**

`[remove] idle-mode-acl {ipv4 | ipv6} access-group acl_name`

**remove**

Removes the specified ACL name from the access group.

`{ipv4 | ipv6} access-group acl_name`

Specifies the ACL type to add to the access group.

- **ipv4**: Specifies that an IPv4 ACL is being added to the access group.
- **ipv6**: Specifies that an IPv6 ACL is being added to the access group.

`access-group acl_name` specifies the name of the ACL being added to the access group as an existing IPv4 or IPv6 ACL name expressed as an alphanumeric string of 1 through 47 characters.

**Usage Guidelines**

Use this command to create a group of ACLs that contain rules to apply to data sent to UEs that are currently in idle mode.

IPv4 ACLs are configured through the Context Configuration Mode using the `ip access-list` command.

IPv6 ACLs are configured through the Context Configuration Mode using the `ipv6 access-list` command.
Examples

The following command configures the APN profile to use an IPv4 ACL named `acl-3-permit` to apply rules to downlink data sent to UEs that are currently in idle mode:

```
idle-mode-acl ipv4 access-group acl-3-permit
```
ip

Defines the IP parameters for this APN profile.

Product

SGSN
S-GW
SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:
[local] host_name (apn-profile-profile_name) #

Syntax Description

ip { qos-dscp { { downlink | uplink } { background forwarding | conversational forwarding | interactive traffic-handling-priority priority forwarding | streaming forwarding } + } | 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 ip 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.

no

Disables the specified IP QoS-DSCP mapping.

qos-dscp

Configures the Differentiated Services Code Point (DCSP) marking to be used for sending packets of a particular 3GPP QoS class.
downlink | uplink

Configures the packets for either downlink (network to subscriber) or uplink (subscriber to network) 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 (THP): 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 must include a DSCP forwarding 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

Forwarding defaults for both uplink and downlink are:

- **conversational** - ef;
- **streaming** - af11;
- **interactive 1** - ef;
- **interactive 2** - af21;
- **interactive 3** - af21;
- **background** - be
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** - deactivate 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** - discard 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 Guidelines**

This command configures a range of IP functions to be associated with the APN profile; such as:

- SGSN/S-GW action in response to detected IP source violations,
- DSCP marking for downlink and uplink configuration per traffic class,
- QoS class diffserv code.

**Examples**

The following command configures the APN profile to instruct the SGSN or S-GW not to check incoming packets for IP source violation information:

```
ip source-violation ignore
```
**ip access-group**

Configure the name of the access control list (ACL) for incoming and outgoing packets.

**Product**
SaMOG

**Privilege**
Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

`configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax Description**

```
[no] ip access-group group_name [ in | out ]
```

- **no**
  If previously configured, removes the IP access group.

- **group_name**
  `group_name` must be an alphanumeric string of 1 to 47 characters.

- **in | out**
  Specify the access group as inbound or outbound.

**Usage Guidelines**

Use this command to configure the ACL name for incoming and outgoing packets to redirect HTTP packets, allow DNS packets and drop other packets. The IP access group specified in this configuration will be used only if the AAA server does not specify the same during authentication.

**Important**

This command is license dependent. Contact your Cisco account representative for more information on SaMOG feature license requirements.

**Examples**

The following command configures an IP access group called `webauthaccgroup` and sets it as inbound:

```
ip access-group webauthaccgroup in
```
ip address pool

Configure the name of the IP address pool from which the IP address needs to be allocated to the user equipment (UE).

Product SaMOG

Privilege Administrator

Command Modes Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax Description

| no | ip address pool name pool_name

no

If previously configured, removes the IP address pool to be used for web authorization.

pool_name

pool_name must be an alphanumeric string of 1 to 31 characters.

Usage Guidelines

Use this command to configure the name of the IP address pool from which the IP address is to be allocated to the UE during the pre-authentication phase. The IP address pool name specified in this configuration will be used only if the AAA server does not specify the same during the pre-authentication phase.

Important This command is license dependent. Contact your Cisco account representative for more information on SaMOG feature license requirements.

Examples The following command configures an IP address pool name of wapool:

ip address pool name wapool
ip context-name

Configure the name of the context where the IP pool configuration needs to be obtained from.

**Product**
SaMOG

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

    configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

**Syntax Description**

- `ip context-name context_name`
- `no ip context-name`

- `no`
  If previously configured, removes the IP context name to be used for web authorization.

- `context_name`
  `context_name` must be an alphanumeric string of 1 to 79 characters.

**Usage Guidelines**
Use this command to configure the name of the context where the IP pool configuration needs to be obtained from and provide the VPN through which the URL to the portal can be reached during the SaMOG web authorization pre-authentication phase, or the data can be offloaded for Local Breakout. If the IP context name is not configured here, and the AAA server does not provide one, the VPN context of the SaMOG service will be used.

---

**Important**
This command is license dependent. Contact your Cisco account representative for more information on SaMOG feature license requirements.

**Examples**
The following command configures the IP context name of *wacxt*

    ip context-name wacxt
**isr-sequential-paging**

Enables or disables the Intelligent Paging for ISR feature.

**Product**
- S-GW
- SAEGW

**Privilege**
- Administrator

**Command Modes**
- Exec > Global Configuration > APN Profile Configuration
- configure > apn-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-*profile_name*)#
```

**Syntax Description**

| remove | isr-sequential-paging |

**remove**

Disables Intelligent Paging for ISR.

**Usage Guidelines**

This command initiates the Intelligent Paging for ISR feature for the specified APN Profile, where paging occurs first towards the last known RAT, then towards the other RAT.

The Intelligent Paging for ISR feature is license dependant. Contact your Cisco account representative for more information.
ipv6

Configures the IPv6 pool name to be used by SaMOG if the 'Framed-IPv6-Pool' AVP is unavailable in the Diameter AA-Answer message, or enable SaMOG to send unsolicited router advertisements (RA) to advertise or deprecate an IPv6 prefix for session with the EoGRE access type.

Product  SaMOG

Privilege  Administrator

Command Modes  Exec > Global Configuration > APN Profile Configuration
  configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local] host_name (apn-profile-profile_name) #

Syntax Description

ipv6 { address prefix-pool pool_name | unsolicited-router-advt { advertise | deprecate } { interval duration
  | num-advts num_advts | num-advts num_advts | interval duration } }

default ipv6 unsolicited-router-advt

no ipv6 { address prefix-pool pool_name | unsolicited-router-advt { advertise | deprecate } }

default

Configures this command to its default value.

no

If previously configured, removes the IP pool name or disables sending unsolicited router advertisements (RA) to advertise or deprecate an IPv6 prefix.

address prefix-pool pool_name

Specify the IPv6 pool name to be used by SaMOG if the 'Framed-IPv6-Pool' AVP is unavailable in the Diameter AA-Answer message.

pool_name must be an alphanumeric string from 1 to 31 characters.

unsolicited-router-advt { advertise | deprecate }

Configure to send unsolicited router advertisements (RA) to advertise or deprecate an IPv6 prefix for session with the EoGRE access type.
**interval duration**
Configure the interval between each unsolicited router advertisement.

*duration* must be an integer from 100 through 16000.
Default: 3000 milliseconds

**num-advts num_advts**
Configure the number of times unsolicited router advertisement must be sent.

*num_advts* must be an integer from 1 through 16.
Default: 3

**Usage Guidelines**
Use this command to:

- Configure the IPv6 pool name to be used by SaMOG if the 'Framed-IPv6-Pool' AVP is unavailable in
the Diameter AA-Answer message. SaMOG uses the configured IPv6 prefix in the Gi context with this
IPv6 pool name.

- Enable SaMOG to send unsolicited router advertisements (RA) to advertise or deprecate an IPv6 prefix
for session with the EoGRE access type.

**Examples**
The following command configures an IPv6 pool name *v6pool*:

```
ipv6 address prefix-pool v6pool
```
local-offload

Enables or disables the SaMOG Local Breakout (LBO) Enhanced, LBO Basic, or Flow-based LBO features.

**Product**
SaMOG

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax Description**

- `local-offload [flow]`
- `no local-offload`

**Usage Guidelines**

Use this command to enable or disable the SaMOG LBO Enhanced, LBO basic, or Flow-based LBO features. When enabled, LBO will be allowed for the UE connecting to the specified SSID, through which this APN profile is reached.

**Important**
The SaMOG LBO features are license dependant. Contact your Cisco account representative for more information.
location-reporting

Configure location change reporting via ULI IE per APN for an S4-SGSN.

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local] host_name (apn-profile-profile_name) #

Syntax Description

location-reporting access-type { gprs | umts }
remove location-reporting access-type { gprs | umts }

remove
Disables the location change reporting definition in the APN profile configuration.

access-type { gprs | umts }
Allows the operator to select location change reporting for the 2G and/or the 3G subscribers. Both access types can be identified in a single command or the command can be issued twice. Either way, two separate entries are created, one for each access type

Usage Guidelines
As with all APN profiles, to enable location change reporting, this APN profile must be associated with a call control profile.

Location change reporting for a Gn-SGSN is enabled with the location reporting command in the Call Control Profile configuration mode. That command can be used to configure the location change reporting function for the S4-SGSN, however that configuration would be over-ridden by an APN profile configuration. As well, using this APN profile location reporting command gives the operator greater control to apply location change reporting per APN.

Examples
Enable location change reporting for 2G subscribers:

location-reporting access-type gprs
**mobility-protocol**

This command allows you to configure the default mobility protocol type to be used for setting up a call when the AAA server forwards an IP address directly.

**Product**
SaMOG

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]\host_name(apn-profile-profile_name)#

**Syntax Description**

mobility-protocol { gtpv1 | gtpv2 | pmip }

no mobility-protocol

no

Removes the mobility protocol configuration for this APN profile.

**Usage Guidelines**

Use this command to configure the default mobility protocol type to be used for setting up a call when the AAA server forwards an IP address directly. If mobility protocol is also configured under the Call Control Profile Configuration Mode, the value configured here will override the configured value in the Call Control profile.

By default, all APN profiles will use the mobility protocol configured under the Call Control Profile Configuration Mode. To configure different mobility protocol values for different APN profiles, use the **mobility-protocol** command in this configuration mode.

**Examples**

The following command configures mobility protocol to GTPv2:

`mobility-protocol GTPv2`
ntsr

This command configures QCI and ARP in the apn-profile for Network Triggered Service Restoration (NTSR).

Product
S-GW

Privilege
Administrator, Security Administrator

Command Modes
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name{apn-profile-profile_name}#

Syntax Description
ntsr { all | qci number arp-priority-watermark number }
no ntsr all
no ntsr qci number arp-priority-watermark number

no
Removes the specified configuration parameters.

ntsr
Enables the network triggered service restoration configuration.

all
Specifies that the NTSR configuration is enabled for all bearers with any qci or arp for MME restoration.

qci
Specifies the Quality of Class Identifier for this NTSR configuration. Must be an integer from 1 to 255.

arp-priority-watermark
Specifies the ARP's priority level watermark value. Must be an integer from 1 to 15.

Usage Guidelines
This command configures qci and arp in the apn-profile for NTSR. The S-GW will decide to retain or release the bearer based on the configured qci/arp, after path failure is detected on ingress side of S-GW. The S-GW can configure a maximum of 2 qci and arp-priority-watermark per apn-profile. The apn-profile can also be configured to retain all bearers from that PDN.
Examples

This example configures the apn-profile to retain all bearers from the PDN.

`ntsr all`
overcharge-protection

Enables overcharge protection for APNs controlled by this APN profile. Each overcharging protection option is a standalone configuration and it does not override the previous option set, if any.

**Product**
S-GW
P-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

```bash
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (apn-profile-profile_name) #
```

**Syntax Description**

```bash
overcharge-protection { abnormal-s1-release | ddn-failure | drop-limit drop_limit_value { packets | bytes } }
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>remove</td>
<td>Removes the specified configuration.</td>
</tr>
</tbody>
</table>

**abnormal-s1-release**
(for future use) If overcharging protection is enabled for abnormal-s1-release, S-GW would send MBR to pause charging at P-GW if Abnormal Release of Radio Link signal occurs from MME.

**Important**
Though the command is available in this release, this scenario is not possible.

**ddn-failure**
If overcharging protection is enabled for ddn-failure message, MBR would be sent to P-GW to pause charging upon receiving DDN failure from MME/S4-SGSN.

**drop-limit drop_limit_value { packets | bytes }**
Send MBR to pause charging at P-GW if specified number of packets/bytes is dropped for a PDN connection.
drop_limit_value is an integer from 1 through 99999.

- **packets**: Configures drop-limit in packets.
- **bytes**: Configures drop-limit in bytes.

**Usage Guidelines**

Use this command to specify P-GW to pause charging on abnormal-s1-release, DDN failure notification, or if the number of packets or bytes dropped exceeds the configured limit.

**Examples**

Use the following command to signal P-GW to pause charging when the number of packets dropped exceeds 1000:

```
overcharge-protection drop-limit 1000 packets
```
pdp-data-inactivity

Configures the APN profile regarding PDP data inactivity. This command is specific to the SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

```plaintext
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name{apn-profile-profile_name}#
```

**Syntax Description**

- `pdp-data-inactivity { action { deactivate | all-pdp | linked-pdp } } | detach-when { all-pdp-inactive | any-pdp-inactive } } | timeout minutes minutes }`:

  - `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.

- `default pdp-data-inactivity { action | timeout }

  - `default`: Resets the APN Profile configuration to the default values for PDP data-inactivity.

  - `no`: Disables the timeout feature of the PDP data-inactivity configuration for this APN profile.

  - `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.
timeout minutes minutes

Specifies the inactivity timeout in minutes. minutes: is an integer from 1 through 1440. Note that even though the timeout is set for minutes, the configuration displays in seconds.

Usage Guidelines

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.

Examples

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 minutes 2
```
pdp-type-ipv4v6-override

Configure the PDP type to use, per APN, if dual PDP type addressing is not supported by the network and the MS/UE requests the IPv4v6 PDP type.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile *profile_name*

Entering the above command sequence results in the following prompt:

[local] *host_name*{apn-profile-*profile_name*}#

**Syntax Description**

`pdp-type-ipv4v6-override { ipv4 | ipv6 }`

`remove pdp-type-ipv4v6-override`

`remove`

Deletes the override configuration and reverts to the default behavior so the SGSN ignores the IPv4v6 request and sends IPv4 to the GGSN.

`ipv4`

Configures IPv4 as the PDP type to send towards the GGSN when overriding the dual PDP type addressing requested by the MS/UE.

`ipv6`

Configures IPv6 as the PDP type to send towards the GGSN when overriding the dual PDP type addressing requested by the MS/UE.

**Usage Guidelines**

This command configures the SGSN to send either IPv4 or IPv6 towards the GGSN when the MS/UE requests PDP type as IPv4v6 but either the SGSN or the RNC is not configured to support dual PDP type.

**Examples**

Use this command to configure the SGSN to always send IPv6, for the PDP type, to the GGSN when overriding a dual PDP type address request from the MS/UE:

`pdp-type-ipv4v6-override ipv6`
pgw-address

Configures the IPv4 and/or IPv6 address of the P-GW supporting the APN associated with this APN profile.

Product
- ePDG
- MME
- SaMOG
- SGSN

Privilege
Administrator

Command Modes
- Exec > Global Configuration > APN Profile Configuration
- configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local] host_name (apn-profile-profile_name) #

Syntax Description

pgw-address ip_address | s5-s8-protocol pmip | { IP-ADDRESS ip_address | primary | secondary | weight weight | primary | secondary | } | fqdn fqdn_var | primary | secondary |

no pgw-address ip_address

no
Disables the P-GW address configured in this APN profile.

ip_address
Specifies the IP address for the P-GW in IPv4 dotted-decimal or IPv6 colon-separated notation.

s5-s8-protocol pmip
MME only. Configures the S5-S8 protocol for the gateway.

primary
Configures the primary PGW for s2b interface.

secondary
Configures the secondary PGW for s2b interface.
fqdn
Configures the FQDN to get the PGW IP address for s2b interface.

weight weight
Specifies the weight (preference) assigned to the addressed P-GW for load balancing. weight is an integer from 1 through 100 where 1 is the least preferred and 100 is the most preferred. If no weight is specified, the P-GW address is assigned a default weight of 1.

If a weight is assigned to an address, the weights of the P-GW(s) (that are operational) are totaled, and then a weighted round-robin selection is used to distribute new primary PDP contexts (for MME) or primary CPC requests (for SGSN) or new PDN connections (for ePDG) among the P-GW(s) according to their weights. As with all weighted round-robin algorithms, the distribution does not look at the current distribution, but simply uses the weights to distribute new requests. For example, two P-GWs assigned weights of 70 and 30 would distribute 70% of calls to one, and 30% to the other. The sum of all weights do not need to total 100.

Usage Guidelines
Use this command to define load balancing to be applied during P-GW selection. A maximum of 16 P-GW addresses can be configured for this APN profile.

On the S4-SGSN, use this command to configure a local P-GW address for operators wishing to bypass DNS resolution of APN FQDN.

Examples
The following command configures the P-GW IP address for this APN profile as 10.2.3.4:

```
pgw-address 10.2.3.4
```
qos allow-upgrade

Configure this command to allow upgrade of QoS from GGSN. The "Upgrade QoS Supported" flag is now set in "Create PDP Context" and "Update PDP Context" messages sent by SGSN. The SGSN signals the availability of this functionality by use of the "Upgrade QoS Supported" bit within the Common Flags IE. The SGSN sets the "Upgrade QoS Supported" bit within the Common Flags IE to "1" within the "Create PDP Context" and "Update PDP Context" procedures.

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:
[local]host_name(apn-profile-profile_name)#

Syntax Description
qos allow-upgrade access-type { gprs | umts } [ prefer-as-cap-subscription ]
remove qos allow-upgrade access-type { gprs | umts }

remove
Removes the support for QoS upgrade from the configuration for this APN profile.

access-type { gprs | umts }
Allows the operator to choose the access type as either "gprs" or "umts" based on whether it is 2G or 3G network scenario.

prefer-as-cap-subscription
Enable this optional keyword to configure capping of QoS with Subscribed QoS (local/HLR). If this keyword is enabled, SGSN accepts a higher QoS in the Create/Update PDP Context Response than sent in Create/Update PDP Context Request, but negotiates and restricts the value within HLR/local subscribed QoS. If this keyword is disabled, the SGSN accepts the QoS in Create PDP Context Response and Update PDP Context Response as the Negotiated QoS (this QoS may be downgraded by the RNC in case of UMTS access).

Usage Guidelines
This command enables the QoS upgrade support feature. On configuring this command, the SGSN sets the "Upgrade QoS Supported" flag within the common flags IE in Tunnel management messages, Create PDP Context Request and Update PDP Context Request messages. The SGSN accepts the QoS from GGSN in
Create PDP Context Response, Update PDP Context Request/Response messages as the Negotiated QoS for the PDP session.

Examples

Use the following command to configure QoS upgrade support in a UMTS scenario:

```
qos allow-upgrade access-type umts prefer-as-cap-subscription
```
qos apn-ambr

Configures the APN-AMBR (aggregate maximum bit rate) that will be stored in the Home Subscriber Server (HSS).

**Product**

MME  
SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration  
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

**Syntax Description**

qos apn-ambr max-ul mbr-up max-dl mbr-dwn  
remove qos apn-ambr

**Syntax Description**

remove

Removes the APN-AMBR changes from the configuration for this APN profile.

**Usage Guidelines**

Use this command to define the MBR that will be enforced by the GGSN or P-GW for both uplink and downlink traffic shaping.

**Examples**

qos apn-ambr max-ul 24234222 max-dl 23423423
**qos class**

Configures local values for the traffic class (TC) parameters for the quality of service (QoS) configured for this APN profile.

**Important**
To enable any of the values/features configured with this command, the qos prefer-as-cap configuration (also in the APN profile configuration mode) must be set to either local or both-hlr-and-local.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax Description**
```
qos class { background | conversational | interactive | streaming } [ qualif_option ]
remove qos class { background | conversational | interactive | streaming } [ qualif_option ]
```

**remove**
Removes previously defined values for the specified option or for an entire class if a qualifying option is not included in the command.

**background**
Selects the background traffic class. This 'best-effort' class manages traffic that is handled as a background function, like email, where time to delivery is not a key factor. The selection of background traffic class can be refined with the addition of one of the following qualifying options:

- **all-values**
- **arp**
- **mbr-down**
- **mbr-map-down**
- **mbr-map-up**
conversational

Selects the 'real-time' conversational traffic class of service, which has the most stringent time requirements of the four classes and is typically reserved for voice traffic. The section of the conversational traffic class can be refined with the addition of one of the following qualifying options:

- all-values
- arp
- gbr-down
- gbr-up
- mbr-down
- mbr-map-down
- mbr-map-up
- mbr-up
- min-transfer-delay
- residual-bit-error-rate
- sdu

All qualifying options are explained below.

interactive

Selects interactive traffic class of service. This class is characterized by a request/response pattern (someone sends data and then waits for a response) which requires the preservation of the data but delivers on a 'best-effort' model. The section of the interactive traffic class can be refined with the addition of one of the following qualifying options:

- all-values
- arp
- mbr-down
- mbr-map-down
- mbr-map-up
- mbr-up
- residual-bit-error-rate
- sdu
- thp
All qualifying options are explained below.

**streaming**

Selects the streaming traffic class of service, which handles one-way, real-time data transmission - such as streaming video or audio. The section of the interactive traffic class can be refined with the addition of one of the following qualifying options:

- **all-values**
- **arp**
- **gbr-down**
- **gbr-up**
- **mbr-down**
- **mbr-map-down**
- **mbr-map-up**
- **mbr-up**
- **min-transfer-delay**
- **residual-bit-error-rate**
- **sdu**

All qualifying options are explained below.

**qualif_option**

Qualifying options are the QoS parameters and they include:

- **all-values** - This option will change the configuration to predefined values for all the relevant QoS parameters for the class. This keyword is not used if other options are to be defined. The predefined values are:

<table>
<thead>
<tr>
<th>QoS Parameter</th>
<th>Predefined Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Class</td>
<td>Background</td>
</tr>
<tr>
<td>SDU delivery order</td>
<td>No</td>
</tr>
<tr>
<td>Delivery of Erroneous SDUs</td>
<td>No</td>
</tr>
<tr>
<td>Max Bit Rate Uplink</td>
<td>64 kbps</td>
</tr>
<tr>
<td>Max Bit Rate Downlink</td>
<td>64 kbps</td>
</tr>
<tr>
<td>Allocation/Retention Priority</td>
<td>3</td>
</tr>
<tr>
<td>SDU Max Size</td>
<td>1500 octets</td>
</tr>
<tr>
<td>QoS Parameter</td>
<td>Predefined Value</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>SDU Error Ratio</td>
<td>3 ((1 \times 10^{-3}))</td>
</tr>
<tr>
<td>Residual Bit Error Rate</td>
<td>4 ((4 \times 10^{-3}))</td>
</tr>
</tbody>
</table>

**Traffic Class**  
**Conversational**

| SDU delivery order                  | No                        |
| Delivery of Erroneous SDUs          | No                        |
| Max Bit Rate Uplink                 | 16 kbps                   |
| Max Bit Rate Downlink               | 16 kbps                   |
| Allocation/Retention Priority       | 3                         |
| Guaranteed Bit Rate Uplink          | 16 kbps                   |
| Guaranteed Bit Rate downlink        | 16 kbps                   |
| SDU Max Size                        | 1500 octets               |
| Minimum Transfer Delay              | 100 milliseconds           |
| SDU Error Ratio                     | 1 \((1 \times 10^{-2})\) |
| Residual Bit Error Rate             | 1 \((5 \times 10^{-2})\) |

**Traffic Class**  
**Interactive**

| SDU delivery order                  | No                        |
| Delivery of Erroneous SDUs          | No                        |
| Max Bit Rate Uplink                 | 64 kbps                   |
| Max Bit Rate Downlink               | 64 kbps                   |
| Traffic Handling Priority           | 3                         |
| SDU Max Size                        | 1500 octets               |
| SDU Error Ratio                     | 3 \((1 \times 10^{-3})\) |
| Residual Bit Error Rate             | 4 \((4 \times 10^{-3})\) |

**Traffic Class**  
**Streaming**

| SDU delivery order                  | No                        |
| Delivery of Erroneous SDUs          | No                        |
| Max Bit Rate Uplink                 | 16 kbps                   |
| Max Bit Rate Downlink               | 16 kbps                   |
**Predefined Value**

<table>
<thead>
<tr>
<th>QoS Parameter</th>
<th>Predefined Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocation/Retention Priority</td>
<td>3</td>
</tr>
<tr>
<td>Guaranteed Bit Rate Uplink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>Guaranteed Bit Rate downlink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>SDU Max Size</td>
<td>1500 octets</td>
</tr>
<tr>
<td>Minimum Transfer Delay</td>
<td>300 milliseconds</td>
</tr>
<tr>
<td>SDU Error Ratio</td>
<td>7 (1 * 10^-3)</td>
</tr>
<tr>
<td>Residual Bit Error Rate</td>
<td>1 (5 * 10^-2)</td>
</tr>
</tbody>
</table>

- **arp** - Sets the allocation/retention priority. Enter an integer from 1 to 3.
- **gbr-down** - Guaranteed Kbps rate for the downlink direction. Enter an integer from the range 1 to 256000.
- **gbr-up** - Guaranteed Kbps rate for the uplink direction. Enter an integer from 1 to 256000.
- **mbr-down** - Maximum Kbps rate for the downlink direction. Enter an integer from the range 1 to 256000.
- **mbr-map-down from** from_kbps **to** to_kbps - Map received HLR MBR (from value) to a locally configured downlink MBR value (to value):
  - from_kbps - Enter an integer from 1 to 25600.
  - to_kbps - Enter an integer from 1 to 25600.
- **mbr-map-up from** from_kbps **to** to_kbps - Map received HLR MBR (from value) to a locally configured uplink MBR value (to value):
  - from_kbps - Enter an integer from 1 to 25600.
  - to_kbps - Enter an integer from 1 to 25600.
- **mbr-up** - Maximum Kbps rate for the uplink direction. Enter an integer from 1 to 256000.
- **min-transfer-delay** - Minimum transfer delay in milliseconds. Enter an integer from 80 to 4000.
- **residual-bit-error-rate** -
  - Background TC 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 TC residual-bit-error-rate range is from 5*10^-2 to 10^-6. Enter one of the following integers, where:
    - 1: represents 5*10^-2
* 2: represents $10^{-2}$
* 3: represents $5*10^{-3}$
* 5: represents $10^{-3}$
* 6: represents $10^{-4}$
* 7: represents $10^{-5}$
* 8: represents $10^{-6}$

* Interactive TC 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 $6*10^{-8}$

* Streaming TC residual-bit-error-rate range is from $5*10^{-2}$ to $10^{-6}$. Enter one of the following integers, where:
  * 1: represents $5*10^{-2}$
  * 2: represents $10^{-2}$
  * 3: represents $5*10^{-3}$
  * 5: represents $10^{-3}$
  * 6: represents $10^{-4}$
  * 7: represents $10^{-5}$
  * 8: represents $10^{-6}$

* sdu - Signalling data unit keyword, 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.

- **thp** - Sets the traffic handling priority. Enter an integer from 1 to 3.

**Usage Guidelines**

This command defines the qualifying options (parameters) for each QoS traffic class defined for this APN profile.

**Important**
Typically this command is only used to define QoS parameters when the APN record does not exist in the subscription record.

Repeat the command as often as needed with different options to define all required QoS criteria. For example, to configure the maximum bit rate (MBR) for the downlink and uplink directions for a traffic class, this command must be used twice, specifying **mbr-down** once and **mbr-up** once.

Advantage for local mapping of MBR: some HLRs cannot be configured with high MBR values. Using the **mbr-map-up** and the **mbr-map-down** parameters allows the SGSN to be configured to treat a specific HLR value as meaning the desired high MBR value. In a case where the HLR does not support HSPA+ bit rates, but the handsets and network do, this feature allows the operator to overcome limitations on the HLR and provide HSPA+ bit rates by overwriting the provisioned HLR-QoS MBR values with SGSN-configured values. When MBR mapping is configured, if QoS is preferred as the HLR value, then the subscription QoS MBR received from the HLR is compared with the "from" value in the table. If it matches, then it is converted to the value specified by the "to" value in the table. QoS negotiation happens based on the converted value.

Advantage for QoS capping with THP and ARP: Controlling THP and ARP via Operator Policy: This functionality can differentiate home vs. roaming subscribers, and prevent visiting subscribers from receiving a high-tiered service. For example, a service provider could offer service differentiation using Ultra/Super/Standard service levels based upon QoS; this could justify charging a corporate customer more to use the Internet APN than would be charged to a consumer. This could be accomplished by controlling the traffic handling priority (THP) over the air interface, i.e. THP 1 = Ultra, THP 2 = Super and THP 3 = Standard.

**Examples**

Use the following command to configure the entire conversational traffic class with predefined QoS options:

```
qos class conversational all-values
```

Now change the background class ARP from 3 to 2:

```
qos class background arp 2
```

Invalidate the THP parameter, by removing all value from the parameter, for the interactive class:

```
remove qos class interactive thp
```
qos dedicated-bearer

Configures the quality of service maximum bit rate (MBR) parameters for the dedicated bearer. This command is specific to the MME.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local] host_name (apn-profile-profile_name)#

**Syntax Description**

qos dedicated-bearer mbr max-ul mbr-up max-dl mbr-dwn

remove qos dedicated-bearer

remove

Removes the dedicated bearer maximum bit rate (MBR) changes from the configuration for this APN profile.

max-ul mbr-up max-dl mbr-dl

Defines the maximum bit rates for uplink and downlink traffic.

- `mbr-up` is an integer from 0 through 1410065408.
- `mbr-dl` is an integer from 0 through 1410065408.

**Usage Guidelines**

Use this command to define the MBRs that will be enforced by the P-GW for both uplink and downlink traffic shaping.

**Examples**

qos dedicated-bearer mbr max-ul 24234222 max-dl 23423423
qos default-bearer

Configures the quality of service parameters for the default bearer. This command is specific to the MME.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

```
[local] host_name{apn-profile-profile_name}#
```

**Syntax Description**

```
qos default-bearer { arp arp_value | preemption-capability { may | shall-not } | vulnerability { not-preemptable | preemptable } } | qci qci
remove qos default-bearer { arp | qci }
```

**remove**

Removes the default bearer QoS configuration from this APN profile.

**arp arp_value**

Defines the address retention priority value. `arp_value` is an integer from 1 through 15.

**preemption-capability { may | shall-not }**

Specifies the preemption capability flag. Options are:

- **may**: Bearer may be preempted
- **shall-not**: Bearer shall not be preempted

**vulnerability { not-preemptable | preemptable }**

Specifies the vulnerability flag. Options are:

- **not-preemptable**: Bearer cannot be preempted.
- **preemptable**: Bearer can be preempted.
`qci qci`

Specifies the QoS Class Identifier for the default bearer profile. `qci` is an integer from 0 through 255.

**Usage Guidelines**

Use this command to set the QoS APR and QCI parameters for the default bearer configuration.

**Examples**

`qos default-bearer arp 2 preemption-capability may`
qos pgw-upgrade

Configures the action to be taken when the MME receives a QoS upgrade from P-GW for default bearers/Non-Guaranteed Bit Rate (Non-GBR) bearers.

Product
MME

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax Description
qos pgw-upgrade non-gbr { accept | reject | locally-cap }
| remove | qos pgw-upgrade non-gbr

remove
Removes the configuration, returning the system to the default setting where the MME accepts the P-GW upgraded QoS values for Non-GBR (default) bearers.

non-gbr { accept | reject | locally-cap }
For Non-GBR (default) bearers, this keyword configures the action the MME takes when it receives a P-GW upgraded QoS value.

• accept: The MME will accept the P-GW upgraded QoS values.
• reject: The MME will reject the P-GW upgraded QoS values.
• locally-cap: The MME compares QCI, ARP and ARP-PVI provided by P-GW to the locally configured values of those parameters. If the values match, then accepts towards the P-GW and use locally configured values towards the UE/RAN for APN-AMBR and ARP-PCI. If the values do not match, the MME rejects the P-GW upgraded QoS values.

Usage Guidelines
Use this command to provide configurability at the APN Profile level for the MME to accept, reject, or locally-cap P-GW upgraded QoS values for default (non-GBR) bearers. This S11 Control is applied whenever QoS parameters are received on S11 interface. The relevant procedures for default bearers are Create Session Response (sent by P-GW during Attach, UE requested PDN connectivity) and Update Bearer Procedures.
(initiated by P-GW resulting from trigger QoS change or other in PCEF/PCRF, or from Modify Bearer Command or Bearer Resource Command sent by MME). **Note:** This configuration is supported only for Default bearers (i.e Non-GBR bearers) in a roaming scenario.

The MME will set the sum of the APN-AMBR of all active APNs up to the value of the subscribed UE-AMBR, subject to the UE-AMBR restriction.

In the case of an Attach Reject or PDN Connectivity Reject, the ESM failure cause "Operator determined barring" is used and the corresponding MME schema bulk statistic is incremented.

In the case of Update Bearer Request Reject, the EGTP cause "Request rejected" is used and the corresponding EGTP bulk statistic is incremented.

A session disconnect reason mme-qos-pgw-upgrade-reject(589) is incremented when QoS upgrade by P-GW is rejected by the MME during initial attach. The corresponding session disconnect reason statistics are incremented.

Refer to the **dedicated-bearers** command to configure QoS controls for dedicated bearers (GBR and Non-GBR).

**Examples**

The following command configures the MME to reject the QOS upgrade from P-GW for non-GBR bearers:

```
qos pgw-upgrade non-gbr reject
```
qos prefer-as-cap

Specifies operational preferences for QoS parameters, specifically QoS bit rates. This command is specific to the SGSN in releases prior to 14.0.

**Product**

MME
SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

**Syntax Description**

qos prefer-as-cap { both-hlr-and-local | both-hss-and-local { local-when-subscription-not-available | minimum | subscription-exceed-reject } | 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**

Instructs the SGSN to use, as the capping value during session establishment, the lower of either the locally configured QoS bit rate or the Home Location Register (HLR) subscription.

**both-hss-and-local { local-when-subscription-not-available | minimum | subscription-exceed-reject }**

For the MME only, specifies the QoS cap value to use.

- **local-when-subscription-not-available**: Use the locally configured values if the Home Subscriber Server (HSS) does not provide any values.
• **minimum**: Use the lower of either the locally configured QoS bit rate or the HSS-provided QoS bit rate.

• **subscription-exceed-reject**: If the requested QoS bit rate exceeds the locally configured value, reject the PDN connection.

**hlr-subscription**

Instructs the SGSN to take the QoS bit rates from the HLR configuration and use the HLR rate as the capping value for session establishment.

Default for SGSN.

**local**

Instructs the SGSN to take the QoS bit rate from the local configuration and use it for session establishment.

**Usage Guidelines**

Use this command to instruct the SGSN or MME to take QoS configuration as the bit rate for session establishment.

The MME has no default setting for this command.

**Examples**

The following command specifies use of the bit rate in subscription at the HLR:

```
qos prefer-as-cap hlr-subscription
```

The following command instructs 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

Configures the actions governing the subscriber traffic flow, if the flow violates or exceeds the configured or negotiated peak or committed data-rates.

This command can be entered multiple times to specify different combinations of traffic direction and class. The SGSN only performs traffic policing if **qos rate-limit direction** is configured.

Additional information on the QoS traffic policing functionality is located in the *System Administration Guide*.

**Product**

SGSN
S-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

*configure > apn-profile profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax Description**

```
qos rate-limit direction { downlink | uplink } [ burst-size { auto-readjust [ duration seconds ] | bytes } ] [ class { background | conversational | interactive traffic_priority | streaming } ] [ exceed-action { drop | lower-ip-precedence | transmit } ] [ gbr-qci [ committed-auto-readjust duration seconds ] ] [ non-gbr-qci [ committed-auto-readjust duration seconds ] ] [ violate-action { drop | lower-ip-precedence | transmit } ] +
remove qos rate-limit direction { downlink | uplink } [ class { background | conversational | interactive traffic_priority | streaming } ]
```

**remove**

Removes the qos rate-limit direction entries from the configuration.

**downlink** | **uplink**

Apply the limits and actions configured with the other keywords to the selected link:

**downlink** - This is the direction from the GGSN or P-GW to the MS.

**uplink** - This is the direction from the MS to the GGSN or the P-GW.
burst-size { auto-readjust | duration seconds | bytes }

Default: See the table of class default values in the Usage section below.

This keyword specifies the peak burst size allowed. System measurements for this value exclude the GTP and outer packet headers. Supported options include:

- **auto-readjust**: This keyword enables dynamic burst-size calculation using negotiated peak data-rate and negotiated committed data-rate.
- **duration seconds**: Must be an integer from 1 to 30; default is 1. 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.
- **bytes**: Must be an integer from 1 to 6000000. This value specifies the static burst size for traffic policing. This option is present for backward compatibility.

**Important**

Use of dynamic burst size (**auto-readjust**) for traffic policing is recommended, rather than the static burst size.

class { background | conversational | interactive traffic_priority | streaming }

The **class** keyword configures the specified traffic policing actions per traffic class, or per traffic priority in the case of interactive traffic class. The following classes are supported:

- **background**: Specifies the traffic action for traffic patterns in which the data transfer is not time-critical (for example, email exchanges).
- **conversational**: Specifies the traffic policing action for traffic patterns in which there is a constant flow of packets in each direction, upstream and downstream.
- **interactive traffic_priority**: Specifies the traffic policing action for traffic patterns in which there is an intermittent flow of packets in each direction, upstream and downstream. 
  
  traffic_priority is the 3GPP traffic handling priority and can be an integer 1,2 or 3.
- **streaming**: Specifies the traffic policing action for traffic patterns in which there is a constant flow of data in one direction, either upstream or downstream.

**Important**

This is an SGSN-specific feature. If this keyword is omitted, the same values are used for all classes.

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
gbr-qci | committed-auto-readjust duration seconds |
Applies the traffic policing policy to guaranteed bitrate bearers.

committed-auto-readjust duration seconds: Must be an integer from 1 to 30. This keyword sets the number of seconds that the committed burst-size calculation will last. This allows the traffic to be throttled to the negotiated rates.

Important This is an S-GW-specific feature.

non-gbr-qci | committed-auto-readjust duration seconds |
Applies the traffic policing policy to non-guaranteed bitrate bearers.

committed-auto-readjust duration seconds: Must be an integer from 1 to 30. This keyword sets the number of seconds that the committed burst-size calculation will last. This allows the traffic to be throttled to the negotiated rates.

Important This is an S-GW-specific feature.

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: Drops the packet
- lower-ip-precedence: Transmits the packet after lowering the IP precedence
- transmit: Transmits the packet

+ This symbol indicates that the keywords can be entered multiple times within a single command.

Usage Guidelines This command configures the APN's quality of service (QoS) traffic policing. Configured actions prevent subscriber flow exceeding or violating configured peak or negotiated 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 APN profile.

Class: Background
<table>
<thead>
<tr>
<th>Class</th>
<th>Uplink Traffic: Disabled</th>
<th>Downlink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Peak Data Rate (in bps): 8640000</td>
<td>Peak Data Rate (in bps): 16000000</td>
</tr>
<tr>
<td></td>
<td>Committed Data Rate (in bps): n/a</td>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td></td>
<td>Burst Size (in bytes): 65535</td>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td></td>
<td>Exceed Action: lower-ip-precedence</td>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td></td>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

Class: Conversational

<table>
<thead>
<tr>
<th>Class</th>
<th>Uplink Traffic: Disabled</th>
<th>Downlink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Peak Data Rate (in bps): 8640000</td>
<td>Peak Data Rate (in bps): 16000000</td>
</tr>
<tr>
<td></td>
<td>Committed Data Rate (in bps): 8640000</td>
<td>Committed Data Rate (in bps): 16000000</td>
</tr>
<tr>
<td></td>
<td>Burst Size (in bytes): 65535</td>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td></td>
<td>Exceed Action: lower-ip-precedence</td>
<td>Exceed Action: lower-ip-precedence</td>
</tr>
<tr>
<td></td>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

Class: Interactive, Traffic Handling Priority: 1

<table>
<thead>
<tr>
<th>Class</th>
<th>Uplink Traffic: Disabled</th>
<th>Downlink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Peak Data Rate (in bps): 8640000</td>
<td>Peak Data Rate (in bps): 16000000</td>
</tr>
<tr>
<td></td>
<td>Committed Data Rate (in bps): n/a</td>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td></td>
<td>Burst Size (in bytes): 65535</td>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td></td>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td></td>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

Class: Interactive, Traffic Handling Priority: 2

<table>
<thead>
<tr>
<th>Class</th>
<th>Uplink Traffic: Disabled</th>
<th>Downlink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Peak Data Rate (in bps): 8640000</td>
<td>Peak Data Rate (in bps): 16000000</td>
</tr>
<tr>
<td></td>
<td>Committed Data Rate (in bps): n/a</td>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td></td>
<td>Burst Size (in bytes): 65535</td>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td></td>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td></td>
<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: Streaming

<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>

**Examples**

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 drops the excess user packets when the subscriber traffic violates both the configured peak and the committed data-rate in the uplink direction. Once either the peak or the committed data-rate for that subscriber goes below the configured/negotiated limit, it transmits them.

```
qos rate-limit direction uplink exceed-action drop
```
**ranap allocation-retention-priority-ie**

Configures the allocation/retention priority (ARP) IE for this APN profile. This command is specific to the SGSN.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

**Syntax Description**

`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 has the highest priority.

`priority` must be an integer from 1 to 3.
class
Configure allocation/retention priority (ARP) 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-not-allowed**
- **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 Guidelines
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, 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 within the ARP IE:

**Table 15: Default ARP Values**

<table>
<thead>
<tr>
<th>Subscribed ARP</th>
<th>Traffic Class</th>
<th>RANAP Priority value</th>
<th>RANAP Preemption Capability</th>
<th>RANAP Preemption Vulnerability</th>
<th>RANAP Queuing Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Conversational</td>
<td>1</td>
<td>not-pre-emptable</td>
<td>0 (not-pre-emptable)</td>
<td>queuing-not-allowed</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>2</td>
<td>0 (not-pre-emptable)</td>
<td>1 (pre-emptable)</td>
<td>queuing-not-allowed</td>
</tr>
</tbody>
</table>
### Examples

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:

```plaintext
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

Configures the activation restrictions of PDP context on the basis of the access type and QoS class.

**Product**

SGSN  
MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration  
configure > apn-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name{apn-profile-*profile_name*}#
```

**Syntax Description**

```
[ no ] restrict access-type { eps | { gprs | umts } | qos-class { background | conversational | interactive | streaming } }  
default restrict access-type { eps | gprs | umts }
```

**no**  
Remove the restriction rules for PDP context activation configured in this APN profile.

**default**  
Resets the restriction rules for PDP context activation to the default values to allow all access types and with QoS class for GPRS and UMTS.

**eps**  
Configures the APN profile to restrict the PDP context activation from EPS (Evolved Packet System) network access.

**gprs**  
Configures the APN profile to restrict the PDP context activation from General Packet Radio Service (2.5G) network access.

**umts**  
Configures the APN profile to restrict the PDP context activation from Universal Mobile Telecommunications Systems (3G) network access.
**qos-class**

Configures the APN profile to restrict the PDP context activation to a specific QoS traffic class. It is optional and can be configured after selecting the network access type. Possible traffic classes options are:

- **background**: Specifies the QoS class as background service session
- **conversational**: Specifies the QoS class as conversational service session
- **interactive**: Specifies the QoS class as interactive service session
- **streaming**: Specifies the QoS class as streaming service session

**Usage Guidelines**

Use this command to configure the restriction rules in an APN profile for activation of PDP context on the basis of the access type. It also provides the facility to restrict type of traffic QoS class.

**Important**

From release 19.0 onwards this command is also supported for MME. In earlier releases this command was supported only on SGSN.

This command is used to configure the APN not supported in particular RAT and PLMN combinations. If this command is enabled, new PDP activations to an APN with which this APN profile is associated are rejected. During handovers PDPs/PDNs are deactivated if the APN name matches with this APN profile.

If the operator does not include the optional QoS-Class keyword option, then complete APN restriction is enabled. And QoS related restrictions have no impact, as QoS restriction is subset of a complete APN restriction.

**Examples**

The following command configures the APN profile to restrict all traffic from a GPRS network service having a QoS class of interactive:

```
restrict access-type grps qos-class interactive
```
sm t3396

The `sm` command includes a new keyword to set the SM T3396 back-off timer for an APN Profile.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

`configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name (apn-profile-profile_name) #
```

**Syntax Description**

```
sm t3396 min minimum_minutes max maximum_minutes cause code
remove sm t3396
```

`remove`

Including this filter with the command removes the SM back-off timer definition from the APN Profile configuration.

`min minimum_minutes`

Enter an integer from 1 to 15 to identify the minimum number of minutes the timer should run; default is 15 minutes.

`max maximum_minutes`

Enter an integer from 1 to 30 to identify the maximum number of minutes the timer should run; default is 30 minutes.

`cause code`

Enter an integer from 1 to 255 to identify the appropriate rejection cause code. The default is 26. During congestion, the configured value is ignored and 26 is sent.

**Usage Guidelines**

- Under congestion, the SGSN can assign the T3396 back-off timers to the UEs and request the UEs not to access the network for a given (timer value) period of time.
• If a message is rejected due to congestion, then the T3396 value will be included in the reject message with cause code 26. The SM back-off timer value sent will be chosen randomly from within the configured T3396 timer value range.

• If T3396 timer value is configured in a APN Profile then it will override the back-off timer values defined for either the SGSN Service or GPRS Service configurations.

**Examples**

Use a command similar to the following to define a T3396 with a timeout range of 2 to 15 minutes.

```bash
sm t3396 min 2 max 15
```
**timeout bearer-inactivity**

Supports a bearer inactivity timeout for GBR and non-GBR S-GW bearer type sessions.

**Product**

S-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local] host_name (apn-profile-profile_name) #

**Syntax Description**

[ remove | timeout bearer-inactivity | gbr | non-gbr ] dur_seconds volume-threshold { total bytes | uplink bytes | downlink bytes } | exclude-default-bearer

**remove**

Removes the timeout bearer-inactivity setting.

**timeout**

Specifies that a session time out value will be configured for this APN profile.

**bearer-inactivity**

Specifies that a session time out value will be configured for this APN profile.

**gbr dur_seconds**

Specifies that the system will check for low activity on a GBR bearer. *dur_seconds* specifies the bearer inactivity timer in seconds. Valid entries are from 900 to 2592000 seconds (15 minutes to 720 hours).

**non-gbr dur_seconds**

Specifies that the system will check for low activity on a non-GBR bearer. *dur_seconds* specifies the bearer inactivity timer in seconds. Valid entries are from 900 to 2592000 seconds (15 minutes to 720 hours).
**volume-threshold**
Specifies that a threshold value of the data traffic for a bearer will be used for the inactivity timeout value.

**total bytes**
Specifies that the total of both uplink and downlink data will be used as a volume threshold. \textit{bytes} must be a value from 1 to 4294967295.

**uplink bytes**
Specifies that an uplink data volume threshold will be used. \textit{bytes} must be a value from 1 to 4294967295.

**downlink bytes**
Specifies that a downlink data volume threshold will be used. \textit{bytes} must be a value from 1 to 4294967295.

**exclude-default-bearer**
Specifies that inactivity handling for the default bearer will be excluded.

**Usage Guidelines**
Use this command to support a bearer inactivity timeout for GBR and non-GBR S-GW bearer type sessions per Qos Class Identifier (QCI). This enables the deletion of bearers experiencing less data traffic than the configured threshold value. This allows for more efficient use of system resources. This feature is supported only for Pure S calls on the SAE-GW.

**Examples**
The following example configures a 5 minute dedicated bearer timeout setting for GBR bearers on a downlink volume threshold of 100000 bytes.

\texttt{timeout bearer-inactivity gbr 300 downlink 100000}
timeout idle

Configures the subscriber's time-to-live (TTL) settings for the EPDG service.

**Product**
ePDG

**Privilege**
System Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Profile Config
configure > apn-profile apn_profile_name

The following prompt is displayed in the APN Profile Config mode:
[local]host_name(apn-profile-profilename)#

**Syntax Description**

```
timeout idle sec { micro-checkpoint-deemed-idle | micro-checkpoint-periodicity }  
no timeout idle
default timeout idle

no
```

Disables idle timeout configuration along with the idle seconds micro-checkpoint duration or deemed idle duration configuration.

```
default
```

Configures the default value for subscriber’s time out settings. The idle timeout default value is 0. The default value of micro-checkpoint-deemed-idle would be 0 seconds and that for micro-checkpoint-periodicity is 10 seconds.

```
idle sec
```

Designates the maximum duration a session can remain idle, in seconds, before system automatically terminates the session. Must be followed by number of seconds between 0 and 2147483647. Zero indicates function is disabled.

```
micro-checkpoint-deemed-idledldur
```

Configures micro-checkpoint duration when UE is deemed idle for this Subscriber. Default is "0" (disabled). dur is an integer between 10 and 1000.
micro-checkpoint-periodicity \textit{dur}

Configures the micro-checkpoint-periodicity for this Subscriber. Default is "10". \textit{dur} is the an integer between 10 and 10000.

\textbf{Syntax Description}

Use this command to configure the subscriber's time-to-live (TTL) settings for the EPDG service.

\textbf{Examples}

The following command configures the idle timeout to 10 and micro-checkpoint-periodicity to 50 for the subscriber:

\texttt{timeout idle 10 micro-checkpoint-periodicity 50}
twan

Configures the APN profile with the default gateway address and mask to be sent in the DHCP offer and PBA messages. This command is specific to SaMOG.

Product
SaMOG

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:
[local]host_name(apn-profile-profile_name)#

Syntax Description
| no | twan default-gateway ipv4/ipv6_address/mask |

no
Removes the default gateway configuration from this APN profile.

ipv4/ipv6_address/mask
Specifies the IP address of the default gateway sent in the DHCP offer and PBA messages for a 3G session. ipv4/ipv6_address must be an IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. mask must be an integer value from 1 to 32 for IPv4 addresses, and 1 to 128 for IPv6 addresses (CIDR notation).

Usage Guidelines
Use this command to configure the APN profile with the default gateway address and mask to be sent in the DHCP offer and PBA messages. This configuration is required for GTPv1 support only. For 3G subscribers, if the configured default gateway is unavailable, or does not match with the subnet of the allocated IP from P-GW or GGSN, the call will be dropped.

A maximum of 16 IP addresses and subnet masks can be configured (in separate lines) for each APN profile.

Examples
The following command configures the APN profile with the default gateway address and mask of 194.122.12.20/12:
twan default-gateway 194.122.12.20/12
virtual-mac

Configures or validates the virtual MAC address for this APN profile to use as the default gateway's MAC address for the user equipment (UE).

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name
Entering the above command sequence results in the following prompt:

(local)host_name(apn-profile-profile_name)#

**Syntax Description**
virtual-mac { mac_address| violation drop }
no virtual-mac [ violation drop ]

no
Removes the virtual MAC configuration from this APN profile.

**mac_address**
Specifies the media-specific access control layer address. `mac_address` must be specified as a 6-byte hexadecimal number with each byte separated by a colon or hyphen, for example, "AA:12:bb:34:f5:0E" or "AA-12-bb-34-f5-0E".

**violation drop**
Specifies SaMOG to validate if the destination MAC address in the packet received over the EoGRE tunnel matches with the configured virtual MAC, broadcast, or multicast address.

**Usage Guidelines**
Use this command to configure or validate the virtual MAC address for this APN profile to use as the default gateway's MAC address for the user equipment (UE).

By default, virtual MAC is not configured. In the event where no virtual MAC is configured, SaMOG creates a virtual MAC by adding `fe:ff` to the start of the bind address of the CGW service.
Important: Dynamic change in the virtual MAC address will only affect new sessions. Older sessions will continue to use the old virtual MAC address until the session exists.

Examples: The following command configures a virtual mac with the IP address of AB:12:22:34:f5:0E for this APN profile:
```
virtual-mac AB:12:22:34:f5:0E
```
virtual-mac
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 an UMTS/LTE service.

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

```plaintext
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)>
```

**Important**

- `aaa`, page 1592
- `access-link`, page 1594
- `accounting-mode`, page 1596
- `active-charging bandwidth-policy`, page 1599
- `active-charging link-monitor tcp`, page 1601
- `active-charging radio-congestion`, page 1603
- `active-charging rulebase`, page 1605
- `active-charging rulebase-list`, page 1607
- `apn-ambr`, page 1609
- `associate accounting-policy`, page 1612
- `associate qci-qos-mapping`, page 1613
- `authentication`, page 1615
- `authorize-with-hss`, page 1620
- `bearer-control-mode`, page 1622
• backoff timer-value, page 1624
• bearer-duration-stats, page 1626
• cc-home, page 1627
• cc-profile, page 1629
• cc-roaming, page 1631
• cc-sgsn, page 1633
• cc-visiting, page 1636
• content-filtering category, page 1638
• credit-control-client, page 1640
• credit-control-group, page 1642
• daf-pdp-type, page 1644
• data-tunnel mtu, page 1646
• data-tunneling ignore df-bit, page 1647
• dcca origin endpoint, page 1649
• dcca peer-select, page 1650
• description, page 1652
• dhcp context-name, page 1653
• dhcp lease-expiration-policy, page 1654
• dhcp service-name, page 1655
• dhcpv6 context-name, page 1656
• dhcpv6 service-name, page 1657
• dns, page 1658
• egtp, page 1660
• egtpc-qci-stats, page 1662
• ehrpd-access, page 1664
• emergency-apn, page 1665
• end, page 1666
• exit, page 1667
• firewall policy, page 1668
• fw-and-nat policy, page 1670
• gsm-qos negotiate, page 1672
• gtpp group, page 1674
• gtpp secondary-group, page 1676
• idle-timeout-activity, page 1678
• ignore-alt-config, page 1679
• ikev2 tsr, page 1681
• ims-auth-service, page 1682
• ip access-group, page 1683
• ip address alloc-method, page 1685
• ip address pool, page 1690
• ip address pool-exhaust-action, page 1692
• ip context-name, page 1693
• ip header-compression, page 1694
• ip hide-service-address, page 1695
• ip local-address, page 1696
• ip multicast discard, page 1697
• ip qos-dscp, page 1698
• ip source-violation, page 1702
• ip user-datagram-tos copy, page 1704
• ipv6 access-group, page 1705
• ipv6 address alloc-method, page 1707
• ipv6 address delegate-prefix-pool, page 1709
• ipv6 address prefix-delegation-len, page 1710
• ipv6 address pool-exhaust-action, page 1711
• ipv6 dns, page 1712
• ipv6 egress-address-filtering, page 1714
• ipv6 initial-router-advt, page 1715
• l3-to-l2-tunnel address-policy, page 1717
• loadbalance-tunnel-peers, page 1719
• long-duration-action detection, page 1721
• long-duration-action disconnection, page 1722
• mbms bmsc-profile, page 1724
• mbms bearer timeout, page 1726
• mbms ue timeout, page 1728
• mediation-device, page 1729
• mobile-ip home-agent, page 1732
• mobile-ip min-reg-lifetime-override, page 1734
• mobile-ip mn-aaa-removal-indication, page 1736
• mobile-ip mn-ha-hash-algorithm, page 1737
• mobile-ip mn-ha-shared-key, page 1738
• mobile-ip mn-ha-spi, page 1739
• mobile-ip required, page 1740
• mobile-ip reverse-tunnel, page 1741
• nai-construction, page 1742
• nbns, page 1744
• network-behind-mobile, page 1746
• nexthop-forwarding-address, page 1748
• npu qos, page 1749
• outbound, page 1751
• paging-policy-differentiation, page 1753
• p-cscf, page 1755
• pco-options, page 1757
• pdn-behavior, page 1759
• pdp-type, page 1761
• permission, page 1763
• pgw fqdn, page 1765
• policy, page 1767
• ppp, page 1769
• proxy-mip, page 1771
• qci, page 1773
• qos negotiate-limit, page 1775
• qos rate-limit, page 1778
• qos-renegotiate, page 1781
• qos traffic-policing, page 1782
• radius, page 1783
• radius group, page 1784
• radius returned-framed-ip-address, page 1785
• radius returned-username, page 1787
• radius rulebase-format, page 1789
- reporting-action, page 1791
- restriction-value, page 1792
- secondary ip pool, page 1794
- selection-mode, page 1795
- stats-profile, page 1797
- timeout, page 1799
- timeout bearer-inactivity, page 1801
- timeout emergency-inactivity, page 1804
- timeout idle, page 1806
- timeout idle micro-checkpoint-deemed-idle, page 1808
- timeout idle micro-checkpoint-periodicity, page 1810
- timeout long-duration, page 1812
- tpo policy, page 1814
- tunnel address-policy, page 1815
- tunnel gre, page 1817
- tunnel ipip, page 1819
- tunnel ipsec, page 1821
- tunnel l2tp, page 1822
- virtual-apn gdc, page 1825
- virtual-apn preference, page 1827
aaa

This command configures Authentication, Authorization, and Accounting (AAA) functionality at the Access Point Name (APN) level.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-apn)#
```

**Syntax Description**

```plaintext
aaa { group aaa_group_name | secondary-group aaa_group_name }
default aaa { group | secondary-group aaa_group_name }
no aaa { group aaa_group_name | secondary-group }
nova
```

- **no aaa**
  - Disables the specified AAA group for the specific APN.

```plaintext
no aaa { group | secondary-group }
```

  - **group**: Uses the default AAA group.
  - **secondary-group**: Removes the secondary AAA group from the APN's configuration.

- **default aaa { group | secondary-group }
  - Configures the default setting for the specified parameter.
    - **group**: Uses the default AAA group—the one specified at the context level or in the APN template.
    - **secondary-group**: Removes the secondary AAA group from the APN configuration.

```plaintext
aaa_group_name
```

- Specifies the AAA server group for the APN.
aaa_group_name must be an alphanumeric string of 1 through 63 characters.

**secondary-group aaa_group_name**
Specifies the secondary AAA server group for the APN.

*aaa_group_name* must be an alphanumeric string of 1 through 63 characters.

### Usage Guidelines

Use this command to configure AAA functionality at the APN level.

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.).

The AAA secondary server group supports the RADIUS Fire-and-Forget feature in conjunction with GGSN for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting acknowledgment from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start / Interim / Stop) sent to the standard AAA RADIUS server.

If the same AAA group is configured with both the **aaa group aaa_group_name** and the **aaa secondary-group aaa_group_name** commands, then this configuration will have no effect and secondary accounting will not happen.

The AAA secondary server group configuration takes effect only when used with APN accounting-mode set to radius-diameter (or) with mediation-acct enabled. The RADIUS accounting triggers for both standard RADIUS accounting and secondary accounting will be taken from the AAA group configured with the **aaa group aaa_group_name** command. On the fly change of this configuration is not supported. Any change to the configuration will have effect only for new calls.

### Examples

The following command applies the AAA server group *star1* to an APN within the specific context:

**aaa group star1**
access-link

Configures IP fragmentation processing over the Access-link (PPP, GTP etc.).

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-apn)>
```

**Syntax Description**

```
access-link ip-fragmentation [{normal | df-ignore | df-fragment-and-icmp-notify}]
default access-link ip-fragmentation
```

**normal**
 Default: Enabled
 Drops the packet and sends an ICMP unreachable message to the source of packet. This is the default behavior.

**df-ignore**
 Default: Disabled
 Ignores the DF (Don't Fragment) bit setting; fragments and forwards the packet over the access link.

**df-fragment-and-icmp-notify**
 Default: Disabled
 Partially ignores the DF bit; fragments and forwards the packet, but also returns an ICMP error message to the source of the packet. The number of ICMP errors sent like this is rate-limited to one ICMP error packet per second per session.

**Usage Guidelines**

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.
Fragmentation may also occur for other reasons, regardless of whether or not fragmentation is performed because of one of the above 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.

**Examples**

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

Configures the protocol to be used for PDP context accounting by this APN.

**Product**
- eWAG
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

`{context_name}host_name(config-apn)#`

**Syntax Description**

In 16.0 and earlier releases:

```
accounting-mode { gtpp | none | radius-diameter | no-early-pdus | | no-interims | }
default accounting-mode
```

In 17.0 and later releases:

```
accounting-mode { gtpp | none | radius | no-early-pdus | | no-interims | }
default accounting-mode
```

default

Restores the command to its default setting.

**gtpp**

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

**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.
In 16.0 and earlier releases, the default value of "accounting-mode gtppp" was not displayed in the "show
configuration" command. The value was only displayed in the output of "show configuration verbose"
command.

In 17.0 and later releases, even for a default configuration of accounting-mode under APN, this will be
indicated in "show configuration" both in verbose and non-verbose modes.

none

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.

radius-diameter

Configures the APN to use RADIUS protocol for accounting purposes. Default: Disabled.

**Important**

The system's RADIUS accounting parameters must be configured prior to using either of the protocols
for accounting. Refer to the radius commands in the Context Configuration Mode Commands and the
AAA Server Group Configuration Mode Commands chapters.

**Important**

The accounting-mode CLI command is used only for RADIUS and GTPP accounting. Hence, in 17.0
and later releases, the keyword option "radius-diameter" has been replaced with radius option, and is
concealed to support backward compatibility.

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.

Configures the GGSN to delay PDUs from/to MS until the RADIUS server returns a response to the GGSN's
accounting START request as per 3GPP standards. The GGSN buffers up to two PDUs per call. Additional
PDUs disable the queuing. On receiving the Accounting response message, the GGSN forwards all the
subsequent PDUs for that call.

**Important**

For StarOS 10.0 and earlier releases, the system buffers up to four PDUs and queues or discards the
remaining PDUs.

**Important**

For StarOS 11.0 and later releases, the system is configured so that none of the PDUs are discarded.

no-interims

Disables the generation of RADIUS interims per APN.

When configured, RADIUS interim updates for this APN will not be sent, regardless of what is configured
in the context that is used for RADIUS accounting.
Different CLI commands are used to disable RADIUS interims for RADIUS accounting and mediation accounting. To disable RADIUS interims for RADIUS accounting, use the following command: `accounting-mode radius no-interims`. To disable RADIUS interims for mediation accounting, use the following command: `mediation-device context-name context_name no-interims`.

**Usage Guidelines**

This command specifies which protocol, if any, will be used to provide accounting for PDP contexts accessing the APN profile.

When the GTPP protocol is used, accounting messages are sent to the charging gateways (CGs) over the Ga interface. The Ga interface and GTPP 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 GTPP version 1. All subsequent CDRs are always fully-qualified partial CDRs. All CDR fields are R4.

If the `radius` option is used, RADIUS 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 the ACS Rulebase Configuration Mode, then both G-CDRs and eG-CDRs would be generated.

**Examples**

The following command configures the APN to use the RADIUSr protocol for accounting:

- `accounting-mode radius`
- `accounting-mode radius no-interims no-early-pdus`
- `accounting-mode radius no-early-pdus no-interims`
active-charging bandwidth-policy

Configures the bandwidth policy to be used for subscribers who use this APN.

Product
ACS
GGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn) #

Syntax Description
active-charging bandwidth-policy bandwidth_policy_name
{ default | no } active-charging bandwidth-policy | fallback-enabled |

default
Configures the default setting.
Default: The default bandwidth policy configured in the rulebase is used for subscribers who use this APN.

no
Disables bandwidth control for the APN.

bandwidth-policy bandwidth_policy_name
Specifies the bandwidth policy name. bandwidth_policy_name must be an alphanumeric string from 1 through 63 characters.

fallback-enabled
Determines whether policy under rulebase can be applied as a fallback value. Fallback is disabled by default.

Usage Guidelines
Use this command to configure bandwidth policy to be used for subscribers who use this APN.
Examples

The following command configures a bandwidth policy named *standard* for the APN:

```
active-charging bandwidth-policy standard [ fallback-enabled ]
```
**active-charging link-monitor tcp**

Enables the TCP link monitoring feature on the Mobile Video Gateway. This command can be configured in either APN Configuration Mode or Subscriber Configuration Mode.

---

**Important**

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

---

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

*configure > context context_name > apn apn_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn) #
```

**Syntax Description**

```
<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
<th>active-charging link-monitor tcp</th>
<th>log</th>
<th>rtt</th>
<th>histogram</th>
<th>time-series</th>
<th>bitrate</th>
<th>histogram</th>
<th>time-series</th>
<th>bitrate</th>
<th>histogram</th>
<th>time-series</th>
</tr>
</thead>
</table>

default
Sets TCP link monitoring to its default value, which is the same as no.

no
Deletes the TCP link monitoring settings and disables TCP link monitoring if previously configured.

**link-monitor tcp**

Enables the TCP link monitoring feature on the Mobile Video Gateway. Note that TCP link monitoring is not enabled by default. Also note that when this command is configured without the log option, TCP link monitoring is enabled without logging, and the output from TCP link monitoring is only used by the dynamic translating feature.

```
log | rtt | histogram | time-series | bitrate | histogram | time-series | rtt | histogram | time-series
```

This option enables statistical logging for TCP link monitoring.
The `rtt` option can be used to enable either `histogram` or `time-series` logging for RTT. Similarly, the `bitrate` option can be used to enable either `histogram` or `time-series` logging for bit rate. When `rtt` and `bitrate` options are used without additional options, histogram and time-series logging are enabled for RTT and/or bit rate respectively.

`-noconfirm`  
Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**  
Use this command to enable TCP link monitoring on the Mobile Video Gateway.

**Examples**  
The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for both RTT and bit rate:  
`active-charging link-monitor tcp log`  
The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for RTT:  
`active-charging link-monitor tcp log rtt`  
The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT:  
`active-charging link-monitor tcp log rtt histogram`  
The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT and time-series logging enabled for bit rate:  
`active-charging link-monitor tcp log rtt histogram bitrate time-series`
**active-charging radio-congestion**

Enables the Congestion Management feature on the Mobile Video Gateway. This command can be configured in either APN Configuration Mode or Subscriber Configuration Mode.

---

**Important**

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

---

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax Description**

```
active-charging radio-congestion policy policy_name
[ default | no ] active-charging radio-congestion policy
```

**default**

Sets congestion management to its default value, which is the same as `no`.

Default: Disabled

**no**

Deletes the settings and disables congestion management if previously configured.

**Usage Guidelines**

Use this command to enable or disable congestion management on the Mobile Video Gateway at either APN or subscriber. As congestion management makes use of the Link Monitoring feature, this must also be enabled along with the congestion monitoring feature.
**Examples**

The following command enables radio congestion for a policy named `test123` for the subscriber:

```
active-charging radio-congestion policy test123
```
**active-charging rulebase**

Specifies the name of the Active Charging Service (ACS) rulebase to be used for subscribers who use this APN.

---

**Important**

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

---

**Product**

ACS  
eWAG  
GGSN  
MVG  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration
`configure > context context_name > apn apn_name`

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

**Syntax Description**

`active-charging rulebase rulebase_name`

`no active-charging rulebase`

- **no**
  
  Removes the rulebase previously configured for this APN.

  **rulebase_name**

  Specifies the name of the ACS rulebase as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to specify the ACS rulebase to be used for subscribers who use the APN.
The following command specifies the ACS rulebase named `rule1` for the APN:

```
active-charging rulebase rule1
```
active-charging rulebase-list

Specifies the name of the ACS rulebase list to be used for subscribers who use this APN.

**Important**

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product**
ACS
GGSN
MVG
P-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration
```
configure > context context_name > apn apn_name
```
Entering the above command sequence results in the following prompt:
```
{context_name}host_name(config-apn)#
```

**Syntax Description**

```
active-charging rulebase-list rulebase_list_name
no active-charging rulebase-list
```

no

If previously configured, removes the rulebase list configured in the APN.

```
rulebase_list_name
```

Specifies the name of the ACS rulebase list.

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

**Usage Guidelines**

Use this command to specify the ACS rulebase list to be used for subscribers who use the APN. The rulebase list is created and configured in the ACS Configuration Mode. For more information, see the `rulebase-list` command in the *ACS Configuration Mode Commands* chapter.
The following command specifies the ACS rulebase list named `rblist` for the APN:

```
active-charging rulebase-list rblist
```

The following command removes the rulebase list named `rblist` from the APN:

```
no active-charging rulebase-list rblist
```
**apn-ambr**

Configures the Aggregated Maximum Bit Rate (AMBR) for all PDNs using this APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

*configure > context context_name > apn apn_name*

Entering the above command sequence results in the following prompt:

\(\text{[context_name]host_name(config-apn)\#}\)

**Syntax Description**

`apn-ambr rate-limit direction \{ downlink | uplink \} \[ burst-size \{ auto-readjust duration milliseconds msecs | seconds 1:30 bytes \} \] \[ violate-action \{ drop | lower-ip-precedence | shape \} \[ transmit-when-buffer-full | transmit \] \[ token-replenishment-interval msecs \] \[ default | no \] 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.

**rate-limit direction \{ downlink | uplink \}**

Specifies that the rate limit is to be applied to either the downlink (network to subscriber) traffic or the uplink (subscriber to network) traffic.

**downlink**: Applies the AMBR parameters to the downlink direction.

**uplink**: Applies the AMBR parameters to the uplink direction.

**burst-size \{ auto-readjust duration milliseconds msecs | seconds 1:30 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: The duration (in seconds) used in this burst size calculation: burst size = peak data rate/8 * auto-readjust duration

seconds must be an integer value from 1 to 30. Default is 1 second.

milliseconds must be an integer value from 100 to 900, in increments of 100 milliseconds. For example, 100, 200, or 300, and so on.

bytes: Specifies the burst size in bytes allowed by this APN for the associated PDNs. It must be an integer from 1 to 4294967295 (1 byte to 4 GB).

Important In 17.3 and later releases, the bytes option has been deprecated.

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: Drops violating packets.

lower-ip-precedence: Sets the DSCP value to zero ("best effort") for violating packets.

shape [ transmit-when-buffer-full ]: Places all violating packets into a buffer and, optionally, transmits the packets when the buffer is full.

Important The shape keyword and optional transmit-when-buffer-full option are available only in StarOS v12.0 and earlier releases, and StarOS v19.2 and later releases.

Important Traffic Shaping is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

transmit: Transmits violating packets. This is the default setting.

token-replenishment-interval

The token replenishment interval is used for both APN AMBR traffic policing and shaping. Operators have the option of using the default interval (100ms) or configuring a lower token replenishment interval of 10ms. Reducing the interval to 10ms helps reduce the queuing time required for the 100ms interval for a given packet size.

Valid entries are 10ms or 100ms.

The default is 100ms.

Important Traffic Shaping is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

Usage Guidelines Use this command to enforce the AMBR for the APN on bearers that do not have a Guaranteed Bit Rate (GBR).
Examples

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
```
**associate accounting-policy**

Associates the APN with specific pre-configured policies configured in the same context.

**Product**
- P-GW
- SAEGW

**Privilege**
Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**

```
[no] associate accounting-policy name
```

- **no**
  Removes the selected association from this APN.

- **name**
  Associates the P-GW APN with an accounting policy configured in the same context. *name* must be an existing accounting policy expressed as a string of 1 through 63 characters.

Accounting policies are configured through the `policy accounting` command in the Context Configuration mode.

**Usage Guidelines**
Use this command to associate the P-GW APN with an accounting policy configured in this context.

**Examples**
The following command associates this P-GW APN with an accounting policy called `acct1`:

```
associate accounting-policy acct1
```
associate qci-qos-mapping

Associates a pre-configured QCI-QoS-Mapping table with this APN to support per APN DSCP marking.

**Product**
P-GW
SAEGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)
```

**Syntax Description**

```
[ no ] associate qci-qos-mapping  qci_qos_map_table_name
```

- **no**
  Removes the selected association of QCI-QoS-Mapping table from this APN.

- **qci_qos_map_table_name**
  Specifies a pre-configured QCI-QoS-Mapping table from global configuration mode to this APN.
  `qci_qos_map_table_name` must be an existing QCI-QoS-mapping table expressed as a string of 1 through 63 characters.

  QCI-QoS-Mapping tables are configured in QCI-QoS_Mapping Configuration mode.

**Usage Guidelines**

Use this command to associate a pre-configured QCI-QoS-Mapping table with an APN to provide per APN basis DSCP marking.

The GGSN/PGW supports configurable DSCP marking of the outer header of a GTP-U tunnel packet based on a QCI/THP table for the Gn/Gp and S5/S8 interfaces. This feature allows configuring DSCP marking table on a per APN basis.

**Important**

In order to be backward compatible with old configuration, if a DSCP marking table is associated with GGSN service and not with the APN, then the one in GGSN service will be used. If table is associated in both GGSN service and APN, then the one on APN will take precedence.
Examples

The following command associates a pre-configured QCI-QoS-Mapping table `dscp_mark_table1` with this APN.

```
associate qci-qos-mapping dscp_mark_table1
```
authentication

Configures the APN's authentication parameters.

**Product**
- GGSN
- P-GW
- PDG/TTG
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

```configure > context context_name > apn apn_name```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**
```
```

default authentication

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 the 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 makes the user name as msisdn or imsi respectively.

username-append-apn
Default: Disabled.
This keyword if enabled, works only with pap and chap options. If username-append-apn option enabled in authentication CLI, then apn name will be appended to the pco received username and same username will be used across all interfaces.

password-use-pco
Default: Disabled.
This keyword, if enabled, uses the password received through Protocol Configuration Options (PCO) from AAA for authentication.

prefer-chap-pco
Default: Disabled.
If this keyword along with msisdn-auth/imsi-auth is enabled, GGSN performs Challenge Handshake Authentication Protocol (CHAP) authentication, if CHAP parameters are received in Protocol Configuration Options (PCO). However, chap username would be constructed as msisdn@apn / imsi@apn and chap challenge, chap response parameters should be used as it is from CHAP parameters received in the PCO IE. If CHAP parameters are not received in the PCO IE of the CPC Request, GGSN does normal Password Authentication Protocol (PAP) authentication with PAP username as msisdn@apn / imsi@apn (ignoring any PAP username if received).

eap initial-access-request
Default: Enabled
Configures the type of initial access request to be used in Diameter EAP (Extensible Authentication Protocol) request. This feature is applicable to only Diameter-based AAA interface and not applicable to RADIUS or any other type of AAA interface.

authenticate-authorize
Default: Enabled
Configures the "authenticate and authorize" type of initial access request to be used in a Diameter EAP request.

authenticate-only
Default: Disabled
Configure the "authenticate only" type of initial access request to be used in a Diameter EAP request.

**allow-noauth**
Default: Enabled
Configures the APN to not perform authentication for PDP contexts as described in the *Usage* section.

**pco-username**
Default: Disabled
This option is used in conjunction with *allow-noauth*. It allows session to get established when PCO contains both pap and chap in authentication disabled case.

**chap preference**
Default: Disabled
Configures the APN to attempt to use CHAP to authenticate the subscriber as described in the *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. It must be an integer from 1 through 1000. The lower the integer, the higher the preference.

**convert-to-mschap**
Default: Disabled
If enabled, the CHAP parameters received with the length of 49 bytes, the AAAmgr converts it to MSCHAP.

**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 the *Usage* section of this command.

_A preference_ can be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. It 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 PAP to authenticate the subscriber as described in the *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. It must be an integer from 1 through 1000. The lower the integer, the higher the preference.

**Usage Guidelines**
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 16: 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 the there was no match and the <strong>aaa constructed-nai authentication</strong> 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 <strong>aaa constructed-nai authentication</strong> 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>
<tr>
<td>chap</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>mschap</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>pap</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 <strong>allow-noauth</strong> parameter is disabled, the system will attempt to use the APN's default username/password specified by the <strong>outbound</strong> 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>msid-auth</td>
<td>Obsolete. Use <strong>imsi-auth</strong>.</td>
<td>Obsolete. Use <strong>imsi-auth</strong>.</td>
</tr>
<tr>
<td>imsi-auth</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>
</tbody>
</table>
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
```
authorize-with-hss

This command enables or disables subscriber session authorization per APN via a Home Subscriber Server (HSS) over an S6b Diameter interface. This feature is required to support the interworking of GGSN with P-GW and HA.

**Product**
P-GW
SAEGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:
```
{context_name}@host_name(config-apn)>
```

**Syntax Description**
```
authorize-with-hss [egtp | s2b | s5-s8 | report-ipv6-addr | lma | s6b-aaa-group aaa-group-name | report-ipv6-addr | report-ipv6-addr]
{default | no} authorize-with-hss
```

default | no

Disables the default authorization of subscriber over S6b interface. Resets the command to the default setting of "authorize locally" from an internal APN authorization configuration.

egtp

Enables S6b authorization for eGTP only.

s2b

Enables S6b authorization for eGTP S2b.

s5-s8

Enables S6b authorization for eGTP S5S8.

lma | s6b-aaa-group aaa-group-name |

Enables S6b authorization for LMA only.
The keyword `s6b-aaa-group aaa-group-name` is used to enable the configuration of AAA group used for S6b authorization in PMIP P-GW.

Two AAA groups are defined within APN configuration, one for RADIUS and another one for Diameter. All the parameters required for RADIUS authentication and accounting will go under `radius_group`. Similarly, Diameter authentication parameters will go under `s6b_group`.

**Important**

If the S6b AAA group is configured under both APN and P-GW service, the APN level configuration takes higher precedence.

**report-ipv6-addr**

Enables the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface.

**Usage Guidelines**

Use this command to enable/disable the authorization support per APN for subscriber over S6b interface, which is used between P-GW and the 3GPP AAA to exchange the information related to charging, GGSN discovery, etc.
bearer-control-mode

Enables or disables the bearer control mode for network controlled QoS (NCQoS) through this APN. It also controls the sending of an IE in GTP messages.

Product
- GGSN
- P-GW
- SAEGW

Privilege
Security Administrator, Administrator

Command Modes
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-apn)#

Syntax Description

bearer-control-mode [ mixed | ms-only | none [ prefer-local-value ] ]
default bearer-control-mode

default
Sets the bearer control mode to default mode of "none".

mixed
Default: Disabled.
This keyword indicates that the 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.

ms-only
Default: Disabled.
This keyword indicates that the bearer will be controlled by the UE side.

none
Default: Enabled.
This keyword indicates that the system will not send any BCM mode information, BCM IE and BCM information in the protocol configuration option (PCO) IE within GTPC messages sent by the GGSN. This option is useful in networks where AGWs or firewalls do not support unknown optional IEs in GTP messages.

**prefer-local-value**

Default: Disabled.

This keyword indicates that the APN configured with "none" option for bearer control mode will not be overridden by any other interface (e.g. Gx interface towards PCRF). As a result it is ensured that BCM IE is never sent in GTP message.

---

**Important**

When bearer control mode is set to "none" with the keyword set "prefer-local-value", even PCRF provided values will not override APN config and therefore sending of BCM mode IE and BCM in PCO IE in CPC Response is supressed.

---

**Usage Guidelines**

Use this command to enable the QoS through bearer control. This can be done either through the MS side or from both the GGSN and MS. To enable network requested QoS user need to enable "Mixed" mode for bearer control.

With this keyword the operator can control sending of BCM information in GTPC messages from the GGSN.

With MS-Only or Mixed options in this mode, the system sends the BCM information element in every Create PDP Context Response and Unknown PDP Context Request and Response message.

In some networks AGWs/Firewall drop/reject GTPC messages if there is an Unknown optional IE. To resolve this, the operator can use the "none" option to control sending of BCM IE and BCM information in the PCO IE within GTPC messages from the GGSN.

**Examples**

The following command enables the bearer control from network and MS side for NCQoS.

```
bearer-control-mode mixed
```
backoff timer-value

Specifies a fixed value and a jitter to introduce randomness in the Backoff Timer value that is returned to the MME for different sessions. This helps prevent a session storm after the Backoff Timer expiry.

---

**Important**
The APN Backoff Timer feature requires that the M2M license be enabled on the P-GW/SAEGW. Contact your Cisco account or support representative for licensing details.

---

**Product**
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-apn)#
```

**Syntax Description**

```
[ no ] backoff timer-value seconds [ jitter seconds ]
```

**no**
Disables the backoff timer values.

**backoff timer-value seconds**
Specifies the backoff timer value, in seconds.
Valid entries are from 0 to 576000 seconds.
There is no default setting.

**jitter seconds**
Specifies the jitter value, in seconds.
Valid entries are from 0 to 1000 seconds.
There is no default setting.
Usage Guidelines
This command must be used with the `pdn-behavior lapi` command in *APN Configuration Mode*.

Examples
The following command specifies a timer-value and jitter setting of 20 seconds:
`backoff timer-value 20 jitter 20`
bearer-duration-stats

Enables or disables per QCI call duration statistics for dedicated bearers.

**Product**

P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

`{context_name}@host_name(config-apn)#`

**Syntax Description**

| no | bearer-duration-stats qci { all |1|2|3|4|5|6|7|8|9 } + |

- **no**
  - Disables per QCI call duration statistics.

- **all**
  - Configures QCI-based duration statistics for all QCI.

- **1|2|3|4|5|6|7|8|9**
  - Configures bearer duration statistics for QCI 1 to 9.

- **+**
  - More than one of the previous keywords can be entered within a single command.

**Usage Guidelines**

Use this command to enable or disable per QCI call duration statistics for dedicated bearers.

**Examples**

The following command enables QCI-based duration statistics for all QCI:

`bearer-duration-stats qci all`
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  
SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration  

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

\[(context_name)host_name(config-apn)\#\]

Syntax Description

c-parameter { behavior bits | profile index }

default cc-home

default

Restores the cc-home parameter to its default setting of the following:

- **behavior bits**: 0x00
- **profile index**: 8

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

Specifies the profile index for the home subscriber charging characteristic. index can be configured to any integer value between 0 and 15. Default: 8
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 Guidelines**

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 ORing the bit strings together and converting 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.

**Examples**

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-profile**

This command selectively enables or disables the Gy sessions based on the Charging Characteristics (CC) profile of the subscriber.

**Product**

GGSN  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration  
`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:  
`(context_name)host_name(config-apn)#`

**Syntax Description**

`cc-profile { cc_profile_index | any } { prepaid-prohibited | credit-control-group cc_group_name }`  
`no cc-profile cc_profile_index`

**no**

This command allows you to specify a CC profile index value. Whatever the CC profile value that was set with `no` command will fall back to "any" CC profile behavior.

Note that this command will not have "any" option. The verbose configuration will display other valid CC profiles and an entry for "any".

**cc_profile_index**

Specifies the CC profile index.  
`cc_profile_index` must be an integer from 0 through 15.  
Note that one charging characteristic value can be mapped to only one credit-control-group/prepaid-prohibited configuration within one APN.

**any**

This keyword is applicable for any non-overridden cc-profile index. This keyword has the least priority over specific configuration for a CC profile value. So, configuring "any" CLI command will not override other specific configurations under APN.
**prepaid-prohibited**

Disables prepaid Gy session for the configured profile index.

**cc_group_name**

Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters. 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.

---

**Usage Guidelines**

Use this command to selectively enable or disable the Gy sessions towards OCS based on the Charging Characteristics (CC) profile of the subscriber. When the prepaid prohibited CLI command is configured, the Gy messages are not triggered for postpaid subscribers. This feature is enabled by default. If APN does not have a specific cc-profile configured, it will fall back to "any" CC profile behavior.

---

**Important**

The existing `credit-control-group` command within APN configuration is obsolete in 17 and later releases. This functionality is available as part of the `cc-profile` command. Also, note that the backward compatibility support exists for the `credit-control-group` CLI command.

The Session controller stores/updating the APN configuration in the AAA manager. During the session setup, the session manager fills the CC value received in session authenticate request, and sends it to AAA manager. The AAA manager matches this against the locally stored APN configuration, and selects the desired credit-control-group/prepaid-prohibited configuration for the session. Then the session manager passes this credit-control-group/prepaid-prohibited information received from the AAA manager to ACS manager.

When the local authentication (session setup request) is done, the credit-control group with the matching charging-characteristic is selected and used. If there is no matching charging-characteristic configuration found for the credit-control group selection, then the default credit-control group for the APN is selected.

The CC based Gy Session Controlling feature is applicable only for the CC value received via GTP-Auth-Request, and during the session establishment. The CC value updated via AAA/PCRF after the session setup will not cause any change in already selected credit-control group. Once the credit-control group is selected after session setup, this feature is not applicable.

---

**Examples**

The following command configures the CC value 2 as prepaid to disable Gy session:

```plaintext
cc-profile 2 prepaid-prohibited
```
**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
- SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

`Exec > Global Configuration > Context Configuration > APN Configuration`

```bash
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn) #
```

**Syntax Description**

`cc-roaming { behavior bits | profile index }
default cc-roaming`

- **default**
  
  Restores the cc-roaming parameter to its default setting of the following:

  - **behavior bits**: 0x00
  - **profile index**: 8

- **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**

  Specifies the profile index for the roaming subscriber charging characteristic. `index` can be configured to any integer value between 0 and 15. Default: 8
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 Guidelines**

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 ORing 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.

**Examples**

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 source for charging characteristics (CC) - those configured locally or those received from the SGSN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:


text

Syntax Description

```plaintext
cc-sgsn { gx-returned | home-subscriber-use-GGSN | radius-returned |
roaming-subscriber-use-GGSN | visiting-subscriber-use-GGSN } +
cc-sgsn { use-GGSN behavior bits profile index[0..15] |
radius-returned { accept-invalid | replace-invalid } | |
gx-returned { accept-invalid | replace-invalid } } )
default cc-sgsn
no cc-sgsn { { radius-returned | home-subscriber-use-GGSN | roaming-subscriber-use-GGSN |
visiting-subscriber-use-GGSN } + | { use-GGSN } | radius-returned { accept-invalid |
replace-invalid } | { gx-returned { accept-invalid | replace-invalid } } )
default 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

**no cc-sgsn**

Causes the GGSN/P-GW 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/P-GW sources of CC.
• roaming-subscriber-use-GGSN
• home-subscriber-use-GGSN
• roaming-subscriber-use-GGSN
• visiting-subscriber-use-GGSN

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 Mode.

home-subscriber-use-GGSN
Configures the GGSN/P-GW to use the locally defined charging characteristics for home subscribers, as configured with the APN Configuration Mode cc-home command.

radius-returned
Configures the GGSN/P-GW to accept Gx returned charging characteristics for all subscribers for the APN.

gx-returned
Configures the GGSN/P-GW to accept charging characteristics returned from the RADIUS server for all subscribers for the APN.

accept-invalid
Configures the GGSN/P-GW to accept charging characteristics returned from PCRF for all subscribers for the APN. It always accepts CC with profile index zero.

replace-invalid
Configures GGSN/P-GW to accept charging characteristics returned from PCRF for all subscribers for the APN, except if CC profile index is zero, it will be replaced with default profile index. Default profile index is 8. This is the default behavior for gx-returned CC.

roaming-subscriber-use-GGSN
Configures the GGSN/P-GW to use the locally defined charging characteristics for roaming subscribers, as configured with the APN Configuration Mode cc-roaming command.

use-GGSN | behavior bits | profile index/ 0...15 /
Configures the GGSN/P-GW 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, the GGSN will use as a source for CCs. The index can be configured to an integer from 0 to 15.

The use-GGSN keyword can be entered alone or in conjunction with the radius-returned keyword. When entered, this keyword overrides the previous configuration using any of the home, roaming, and/or visiting keywords.
visiting-subscriber-use-GGSN
Configures the GGSN/P-GW to use the locally defined charging characteristics for visiting subscribers, as configured with the APN Configuration Mode cc-visiting command.

+

More than one of the above keywords can be entered within a single command.

Usage Guidelines
This command specifies whether or not CCs received from the SGSN will be accepted. If they are not accepted, the GGSN/P-GW will use those that have been configured locally.

The GGSN/P-GW'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/P-GW is located.
- **Roaming**: Subscribers that are serviced by a SGSN belonging to a different PLMN than the one on which the GGSN/P-GW is located.
- **Visiting**: Subscribers belonging to a different PLMN than the one on which the GGSN/P-GW is located.
- Any subscriber in the APN.

Examples
The following command instructs the GGSN/P-GW to accept CCs for any subscriber in the APN based on local profile configurations of CCs.

```
cc-sgsn use-GGSN profile x
```

Assuming the CC source as defined with the previous command, the following command instructs the GGSN/P-GW to accept CCs supplied by the SGSN(s) and disables the acceptance of CCs supplied by the GGSN/P-GW for any subscriber within the APN:

```
no cc-sgsn use-GGSN
```

The following command instructs the GGSN/P-GW 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.

```
cc-sgsn radius-returned
```

The following command disables the acceptance of CCs supplied by the GGSN/P-GW for visiting and roaming subscribers:

```
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
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-apn)>
```

**Syntax Description**

```
cc-visiting behavior bits profile index
default cc-visiting
```

**default**

Restores the cc-visiting parameter to its default setting of the following:

- **behavior bits**: 0x00
- **profile index**: 8

**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**

Specifies the profile index for the visiting subscriber charging characteristic. *index* can be configured to any integer value between 0 and 15. Default: 8
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 Guidelines**

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 ORing 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.

**Examples**

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

Enables or disables the specified pre-configured Category Policy Identifier for Category-based Content Filtering support.

Product CF

Privilege Security Administrator, Administrator

Command Modes 
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

\[(context_name)host_name(config-apn)#

Syntax Description
content-filtering category policy-id cf_policy_id

no

disables the previously configured category policy identifier for Content Filtering support to the APN. This is the default setting.

policy-id cf_policy_id

Applies the specified content filtering category policy ID, configured in the ACS Configuration Mode, to this APN.

cf_policy_id must be a category policy ID entered as an integer from 1 through 4294967295.

If the specified category policy ID is not configured in the ACS 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 the ACS Rulebase Configuration Mode.

Usage Guidelines
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 the ACS Rulebase Configuration Mode determines the policy.

Up to 64 different policy IDs can be defined.

Examples

The 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
```
credit-control-client

Configures the credit-control client parameters for subscribers who use this APN.

**Product**
- GGSN
- HA
- IPSG
- PDSN
- P-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
{context_name}\host_name\(config-apn)#
```

**Syntax Description**

```
credit-control-client { event-based-charging | override session-mode { per-sub-session | per-subscriber } }
no credit-control-client { event-based-charging | override session-mode }
default credit-control-client event-based-charging

no
Disables the configured setting.

default
Resets the command to its default setting of disabled.

event-based-charging
Enables event-based charging.

override session-mode { per-sub-session | per-subscriber }
```

Overrides the session-mode configured through the CLI command "require ecs credit-control session-mode per-subscriber" in Global Configuration mode so that different APN can operate in different modes. For example, one APN can be configured to work in per-subscriber mode, while another in per-sub-session mode.
This keyword is used to switch between subscriber level Gy and sub-session level Gy.

**Important** This CLI can be changed on the fly. The modified values will be reflected only in the new subscriber session.

The `no` command removes the override CLI and makes the APN fall back to the configuration specified through the CLI command "require ecs credit-control session-mode per-subscriber".

**Usage Guidelines** Use this command to configure the credit-control client parameters for this APN.

This configuration should be enabled to report UE’s PLMN, time zone and ULI changes through Event-based-Gy session. In the event that both Gy Online charging and Gy event reporting are enabled, the P-GW shall send only CCR-Update requests to the OCS and shall not send CCR-Event requests.

With the inclusion of this keyword `override session-mode` ... in 14.1 release, it is possible to seamlessly change the configuration from bearer level to APN level and vice-versa without requiring a system reboot.

**Examples** The following command enables event-based Gy support for the current APN: `credit-control-client event-based-charging`
credit-control-group

Configures the credit control group to be used for subscribers who use this APN.

This command is obsolete in 17 and later releases. The functionality of this command is available as part of the cc-profile command in the APN Configuration mode. Refer to the cc-profile command in this chapter.

**Product**
- GGSN
- ACS
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-apn)#
```

**Syntax Description**

```
credit-control-group cc_group_name | cc-profile cc_profile_index |
no credit-control-group | cc_group_name cc-profile cc_profile_index |
```

```
no
```

Removes the previously configured credit control group from the APN configuration.

```
cc_group_name
```

Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters.

**Important**
Release 16 onwards, a maximum of up to four credit-control-group - charging-profile configurations are possible within one APN.
**cc-profile cc_profile_index**

Specifies the charging-characteristic preference for the credit-control-group.

For example, 1 for Hot Billing, 2 (Flat Rate), and 8 (Post-Paid)

`cc_profile_index` must be an integer from 0 through 15.

Note that one charging-characteristic value can be mapped to only one credit-control-group inside one APN.

---

**Important**

The CLI command "cc-sgsn" within APN configuration mode, should be used cautiously as this will cause the charging-chars to be altered/modified.

---

**Usage Guidelines**

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.

In releases prior to 16, only one credit-control-group can be specified inside an APN. In 16 and later releases, the APN configuration is extended to include the Charging-Characteristic (CC) preference for the credit-control-group. This APN configuration is also extended to allow configuring additional credit-control-groups for each of the CC values. With this enhancement, the OCS selection can be done based on the CC value received via GTP request.

When the local authentication (session-setup-request) is done, the credit-control-group with the matching charging-characteristic will be selected, and used. If there is no matching charging-characteristic configuration found for the credit-control-group selection, then the default credit-control-group for the APN will be selected.

The CC based OCS selection feature is applicable only for the Charging-Chars value received via GTP-Auth-Request, and during the session-establishment. The Charging-Chars value updated via AAA/PCRF after the session setup will not cause any change in already selected "credit-control-group". Once the credit-control-group is selected (after session setup), this feature is not applicable.

APN configuration information is stored in AAA manager. Credit control group information from the APN configuration is filled during the session-authentication time, by AAA manager. So, AAA manager should be informed of the Charging-Characteristic value received at the time of Session-Authentication, so that the desired credit-control-group can be selected.

Thus, the operator has the added flexibility to choose different OCS charging servers based on their business logic. This could help multi-national operators to choose correct OCS servers based on countries for roaming subscribers.

---

**Examples**

The following command configures a credit control group named `testgroup12` for the current APN:

```
credit-control-group testgroup12
```
daf-pdp-type

By configuring this command P-GW/GGSN can set different behavior of assigning PDN Type and return cause code when request for ipv4v6 PDN with DAF bit False is received.

**Product**
- GGSN
- P-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-apn)#

**Syntax Description**

daf-pdp-type {ipv4 | ipv6} cause-code { network-preference | single-address-bearer-only }

daf-pdp-type
- Configures PDP type for requested IPv4v6 PDN with Dual Address Flag zero. Default PDP type is IPv6.

ipv4
- Configures PDP type for this APN to be IPv4.

ipv6
- Configures PDP type for this APN to be IPv6

ipv6
- Configures PDP type for this APN to be IPv6.

cause-code
- Configures GTP cause code for requested IPv4v6 PDN with Dual Address Flag zero. Default GTP cause code is single-address-bearer-only.

network-preference
- New PDP type due to network preference.
**single-address-bearer-only**

New PDP type due to single address bearer only.

**Usage Guidelines**

By configuring this command P-GW/GGSN can set different behavior of assigning PDN Type and return cause code when request for ipv4v6 PDN with DAF bit False is received. If this command is not configured P-GW/GGSN it uses the default option of assigning ipv6 pdn type with return cause of 'New PDN Type due to single address bearer only'.

**Examples**

The following command configures PDP type and GTP cause code for requested IPv4v6 PDN due to network preference.

```
daf-pdp-type ipv4 cause-code network-preference
```
**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  
SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration  
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

{(context_name)host_name}(config-apn) #

**Syntax Description**

data-tunnel mtu bytes  
default data-tunnel mtu

**default**

Returns the command to the default value of 1500.

**bytes**

Specifies the MTU for the IPv6 tunnel between the P-GW and the mobile node. bytes must be an integer between 1280 and 2000. Default: 1500

**Usage Guidelines**

Use this command to set the MTU for data traffic on the IPv6 tunnel between the P-GW and the mobile node.

**Examples**

The following command sets the MTU for IPv6 data traffic to 1400 bytes:

data-tunnel mtu 1400
**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
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

`[(context_name)host_name](config-apn)#`

**Syntax Description**

```
| default | no | data-tunneling ignore df-bit |
```

- **default**
  Restores the data-tunneling parameter to its default setting of disabled.

- **no**
  Disables this option. The DF bit in the tunneled IP packet header is not ignored during tunneling. This is the default setting.

- **ignore df-bit**
  Ignores the DF bit in the tunneled IP packet header during tunneling. This is the default setting.

**Usage Guidelines**

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.
Examples

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
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
- ACS
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-apn)#
```

**Syntax Description**

- `dcca peer-select peer host_name { realm realm_name } { secondary-peer host_name }`
- `no dcca peer-select`

**no**

Removes the previously configured Diameter credit control peer selection.

- `host_name`
  Specifies a unique name for the peer as an alphanumeric string of 1 through 63 characters that allows punctuation marks.

- `realm realm_name`
  Specifies the realm as an alphanumeric string of from 1 through 127 characters that allows punctuation marks. The realm may typically be a company or service name.

- `secondary-peer host_name`
  Specifies a back-up host that is used for fail-over processing as an alphanumeric string of from 1 through 63 characters. When the route-table does not find an AVAILABLE route, the secondary host performs fail-over processing.
**Usage Guidelines**

Use this command to select a Diameter credit control peer and realm.

**Important**

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.

**Examples**

The following command selects a Diameter credit control peer named test and a realm of `companyx`:

```
dcca peer-select test realm companyx
```
**description**

Allows you to enter descriptive text for this configuration.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

- `description text`
- `no description`

  **no**

  Clears the description for this configuration.

  **text**

  Enter descriptive text as an alphanumeric string of 1 to 100 characters.
  If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA B BBB".

**Usage Guidelines**

The description should provide useful information about this configuration.
**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
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration
```
configure > context context_name > apn apn_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-apn)#
```

**Syntax Description**
```
[ no ] dhcp context-name name
```

- **no**
  Removes a previously configured context name.

- **name**
  Specifies the name of a context configured on the system in which one or more DHCP services are configured. 
  name is an alphanumeric string of 1 through 79 characters that is case sensitive.

**Usage Guidelines**
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.

**Examples**
The following command configures the APN to look for DHCP services in a context called dhcp-ctx:
```
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
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-apn)#
```

**Syntax Description**
- `dhcp lease-expiration-policy { auto-renew | disconnect }`
- `default dhcp lease-expiration-policy`

**default**
Restores the dhcp lease-expiration-policy parameter to its default setting of auto-renew.

**auto-renew**
Configures the system to automatically renew an IP address' lease when it is about to expire for PDP contexts facilitated by the APN. Default: Enabled

**disconnect**
Configures the system to automatically release the PDP context when the lease for the IP address associated with that context expires. Default: Disabled

**Usage Guidelines**
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.

**Examples**
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
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration
```
configure > context context_name > apn apn_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-apn)#
```

**Syntax Description**

```
[ no ] dhcp service-name service_name
```

- **no**
  Removes a previously configured DHCP service name.

- **service_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 an alphanumeric string of 1 through 63 characters that is case sensitive.

**Usage Guidelines**
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 `dhcp context-name` command.

**Examples**
The following command instructs the APN to use a DHCP service called `dhcp1`:
```
dhcp service-name dhcp1
```
**dhcpv6 context-name**

Configures the name of the context on the system in which DHCPv6 functionality is configured. If a DHCPv6 service is configured in the APN, this DHCPv6 context name is used to get an address.

**Product**
- GGSN
- P-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
<context_name>host_name>(config-apn)#
```

**Syntax Description**

- `dhcpv6 context-name ctx_name`
- `{ no } dhcp context-name`

- **no**
  - Removes a previously configured context name.

- `ctx_name`
  - Specifies the name of a context configured on the system in which one or more DHCPv6 services are configured. `ctx_name` is an alphanumeric string of 1 through 79 characters that is case sensitive.

**Usage Guidelines**
If the APN is to support dynamic address assignment via DHCPv6, 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 DHCPv6 services are configured.

The command can be used to identify a single DHCPv6 service instance within the specified context to use to facilitate the address assignment.

**Examples**

The following command configures the APN to look for DHCPv6 services in a context called `dhcpv6-ctx`:

```
dhcpv6 context-name dhcpv6-ctx
```
**dhcpv6 service-name**

Specifies which DHCPV6 service to use, if the alloc-type is configured as dhcpv6-client or dhcpv6-relay.

**Product**
- GGSN
- P-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**

```
[ no ] dhcpv6 service-name service_name
```

- **no**
  - Removes a previously configured DHCPv6 service name.

- **service_name**
  - Configures the name of the DHCPv6 service instance that is to be used by the current APN for the dynamic assignment of IPv6 addresses to PDP contexts. The name can be an alphanumeric string of 1 through 63 characters that is case sensitive.

**Usage Guidelines**

Use this command to specify a pre-configured DHCPv6 service instance that is to be used by the APN for IPv6 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 `dhcpv6 context-name` command.

**Important**

Only one DHCPv6 service can be configured for an APN

**Examples**

The following command instructs the APN to use a DHCPv6 service called `dhcpv6_svc`:

```
dhcp service-name dhcpv6_svc
```
**dns**

Configures the Domain Name Service (DNS) servers that will be used by the APN for PPP.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**

```
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-apn)#
```

**Syntax Description**

```
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**
  Configures the IP address of the DNS server expressed in IPv4 dotted-decimal notation.
  Default: primary = 0.0.0.0, secondary = 0.0.0.0

- **dns_address**
  Specifies the IP address of the DNS server to remove, expressed in IPv4 dotted-decimal notation.
Usage Guidelines

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 (NetBIOS Name Service) servers to be negotiated via ICPC (Initial Connection Protocol Control) with the LNS (L2TP Network Server).

Examples

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
```
egtp

Enables/disables the Overcharging Protection feature on an APN service.

Product

P-GW
SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:
{context_name}host_name{config-apn}#}

Syntax Description

egtp overcharge-protection [ drop-all | transmit-all ]
{ default | no | remove } egtp overcharge-protection

default
Disables overcharging protection.

no
Disables overcharging protection.

remove
Removes overcharging protection configuration.

overcharge-protection [ drop-all | transmit-all ]
drop-all: Configures overcharging protection to drop all packets received in LORC.
transmit-all: Configures overcharging protection to send all packets received in LORC mode to S-GW.

Usage Guidelines

Use this command to enable/disable the Overcharging Protection feature on an APN service.

When Overcharging Protection feature is configured at both P-GW service and APN, configuration at APN takes priority.
Use of Overcharging Protection feature requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

Examples

The following command configures overcharging protection to drop all packets received in LORC

```
egtp overcharge-protection drop-all
```
egtpc-qci-stats

Enables/disables an APN candidate list for the apn-expansion bulkstats schema.

Product

P-GW
SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-apn)#

Syntax Description

| no | egtpc-qci-stats { all | qci1 | qci2 | qci3 | qci4 | qci5 | qci6 | qci7 | qci8 | qci9 } |

default

Disables an APN candidate list for the apn-expansion bulkstat schema.

no

Disables APN candidate list(s) for the apn-expansion bulkstat schema.

all

Configure apn-qci-egtpc statistics for all QCI.

qci1

Configure apn-qci-egtpc statistics for QCI 1.

qci2

Configure apn-qci-egtpc statistics for QCI 2.

qci3

Configure apn-qci-egtpc statistics for QCI 3.

Configure apn-qci-egtpc statistics for QCI 5.


More than one of the above keywords can be entered within a single command.

Usage Guidelines
Use this command to enable/disable an APN candidate list for the APN Expansion bulkstats schema. You can enable which APN collects granular statistics using this configuration. In those granular statistics, it is possible to decide which particular statistics to collect.

Caution
Supporting more granular statistics/bulkstats on APN (up to 12 APNs are supported) has an impact on system performance. Statistics need to be obtained at regular intervals for a few minutes. Each of these retrievals can lead to gigabytes of information being gathered and consolidated. Due to this issue, granular bulkstats collection is restricted/controlled.

Examples
The following command configures all QCI bulkstats in the apn-expansion schema.

`egtpc-qci-stats all`
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
SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-apn) #

Syntax Description

[ default | no ] ehrpd-access drop-ipv6-traffic

| default | no |
Reset this command to its default setting of disabled.

drop-ipv6-traffic

Excludes IPv6 traffic from being delivered to UEs, accessing PDNs from the eHRPD network that do not have IPv6 capabilities.

Usage Guidelines

Use this command to exclude IPv6 traffic from being delivered to UEs on the eHRPD network that do not have IPv6 capabilities.
emergency-apn

Configures this APN as an emergency APN for Voice over LTE (VoLTE) based E911 support.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**

[ default | no ] emergency-apn

[ default | no ]

Resets this command to its default setting of disabled.

**Usage Guidelines**

Use this command to configure this APN as an emergency APN for VoLTE based E911 support. With this support, a UE is able to connect to an emergency PDN and make Enhanced 911 (E911) calls while providing the required location information to the Public Safety Access Point (PSAP).

E911 is a telecommunications-based system that is designed to link people who are experiencing an emergency with the public resources that can help. This feature supports E911-based calls across the LTE and IMS networks. In a voice over LTE scenario, the subscriber attaches to a dedicated packet data network (PDN) called EPDN (Emergency PDN) in order to establish a voice over IP connection to the PSAP. Both signaling and RTP media flow over a dedicated emergency bearer. Additionally, different than normal PDN attachment that relies on AAA and PCRF components for call establishment, the EPDN attributes are configured locally on the P-GW, which eliminates the potential for emergency call failure if either of these systems is not available.
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

dend

Usage Guidelines

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 Description
exit

Usage Guidelines
Use this command to return to the parent configuration mode.
firewall policy

Enables or disables Stateful Firewall support for the APN.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-apn)#

Syntax Description

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

Usage Guidelines

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 ACS Rulebase Configuration Mode.

Important

Unless Stateful Firewall support for this APN is enabled using this command, firewall processing for this APN is disabled.
If firewall is enabled, and the rulebase has no firewall configuration, Stateful Firewall will cause all packets to be discarded.

**Examples**

The following command enables Stateful Firewall support for an APN:

```
firewall policy firewall-required
```

The following command disables Stateful Firewall support for an APN:

```
no firewall policy
```
fw-and-nat policy

Specifies the Firewall-and-NAT policy to be used for subscribers who use this APN.

Product
- eWAG
- PSF
- NAT

Privilege
- Security Administrator, Administrator

Command Modes
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-apn)#
```

Syntax Description
```
fw-and-nat policy fw_nat_policy
{ default | no } fw-and-nat policy

default
Configures the default setting.
Default: The default Firewall-and-NAT policy configured in the rulebase is used for subscribers who use this APN.

no
Disables Firewall and NAT for the APN.

fw_nat_policy
Specifies the Firewall-and-NAT policy for the APN as an alphanumeric string of 1 through 63 characters. Note that this policy will override the default Firewall-and-NAT policy configured in the ACS rulebase.

Usage Guidelines
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.
This command is customer-specific and is only available in StarOS 8.1.

Important

This customer-specific command must be used to configure the Policy-based Firewall-and-NAT feature.

Important

Examples

The following command configures a Firewall-and-NAT policy named \textit{standard} for the APN:

\texttt{fw-and-nat policy standard}
gsm-qos negotiate

Enables negotiation of the QoS Reliability Class attribute 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
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-apn)#
```

**Syntax Description**

```
gsm-qos negotiate sdu-error-ratio  sdu-error-ratio-code  [ residual-ber residual-ber-code ]
[ ]
```

**no**
Disables negotiation of the QoS Reliability Class attribute.

```
sdu-error-ratio  sdu-error-ratio-code
```

Enables the negotiation of the QoS Reliability Class attribute based on Service Data Unit (SDU) Error Ratio attributes. `sdu-error-ratio-code` corresponds to distinct SDU Error ratio values within an integer range of 1 to 7.

```
residual-ber  residual-ber-code
```

Enables the optional configuration of negotiation of the QoS Reliability Class attribute based on Residual Bit Error Ratio (BER) attributes. `residual-ber-code` corresponds to distinct Residual Bit Error Ratio values within an integer range of 1 to 9.

**Usage Guidelines**
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>
<tr>
<td>6</td>
<td>10-6</td>
</tr>
<tr>
<td>7</td>
<td>10-1</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*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*10-2</td>
</tr>
<tr>
<td>2</td>
<td>10-2</td>
</tr>
<tr>
<td>3</td>
<td>5*10-3</td>
</tr>
<tr>
<td>4</td>
<td>4*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*10-8</td>
</tr>
</tbody>
</table>

**Examples**

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

Enables a configured GTPP server group to an APN for CGF accounting functionality.

Important

In releases prior to 11.0, only one GTPP group is allowed to be configured per APN. Releases 11.0 through 15.0, this CLI can be used to configure up to a maximum of 32 GTPP groups. In 16.0 and later releases, this CLI allows the user to configure only up to six GTPP groups.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-apn)#

Syntax Description

gtpp group group_name [ accounting-context ac_context_name ]
default gtpp group
no gtpp group group_name

no
Removes all the configured GTPP groups for the specific APN.

group_name
Specifies the name of server group that is used for authentication/accounting for specific APN. group_name must be an alphanumeric string of 1 to 63 characters. It must be identical to the one configured earlier within the same APN context.

Important

In Release 11.0 and later, if you have mistakenly configured a GTPP group, you should remove the initially configured group and configure the new desired group. However, in Releases prior to 11.0, there is no need to remove the incorrect configuration; instead you can directly reconfigure the desired GTPP group.
If a GTTP group entry is invalid, this GTTP group will be ignored and the next valid GTTP group in the APN will be used. If no valid GTTP group exists, then the default GTTP group in the accounting context specified by the GGSN service will be used.

Important

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 must be an alphanumeric string of 1 through 79 characters that is case sensitive.

Note that if an accounting context is not specified here, the system uses the GGSN service context or the context configured by the accounting context command in the GGSN Service Configuration mode.

Usage Guidelines

This feature provides the GTTP server configuration parameters under a GTTP group node. Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual an GTTP server group for subscribers in that context. Each server group consists of a list of CGF (Charging Group Function) accounting servers.

In case no GTTP group is applied for the said APN or default APN template, then the default GTTP server group available at the context level is applicable for accounting of a specific APN.

Important

When multiple GTTP groups are applied to the same APN, the load will be shared across these GTTP groups. Sessions for this APN will use all the configured GTTP groups in a round robin fashion.

Once a GTTP group is selected for a subscriber session, the GTTP group will never change under any circumstances. A request is initially sent to primary CGF server configured in that group. When the primary fails to respond, the request is sent to secondary CGF server.

The process of failover from primary to secondary is per the 3GPP standards. Multiple GTTP groups configuration is actually supported only for load sharing of sessions within an APN and not used for failover. When all CGFs are down in a GTTP group, the requests are archived either in hard disk or main memory depending on whether or not streaming is enabled.

The AAA proxy allocates a lot of memory on a per GTTP group basis statically regardless of the usage. So if the number of GTTP groups is reduced to around 3 then the issue with the AAA proxy going to warn memory state will not be observed.

In releases prior to 16.0, up to a maximum of 32 GTTP groups were allowed to be configured per APN. In 16.0 and later releases, there is a limit of configuring only up to six GTTP groups per APN. In case customers are using more than six GTTP groups, the AAAPProxy will use more memory than is supported and will be in "warn" state of memory. With the reduction in the number of GTTP groups configured, there will no CDR loss due to AAA proxy kill as CDRs are archived in AAA manager when AAA proxy goes to warn state.

Examples

The following command applies a previously configured GTTP server group named star1 to an APN within the specific context:

gtpp group star1

The following command disables the applied GTTP server group for the specific APN:

no gtpp group star1
gtpp secondary-group

Enables or associates a pre-configured secondary GTPP server group to an APN for CGF (Charging Group Function) accounting functionality. By default it is disabled.

Product
- GGSN
- P-GW
- SAEGW

Privilege
Security Administrator, Administrator

Command Modes
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

\[(context_name)host_name(config-apn)\#\]

Syntax Description
- \texttt{gtpp secondary-group group_name [ accounting-context actt_ctxt_name ] [ default \textbar no ] gtpp secondary-group group_name}

- \texttt{default}
  - Default: Enabled
  - Restores the default mode for secondary GTPP group for APN template.

- \texttt{no}
  - Disables the configured/associated GTPP secondary group for specific APN.

- \texttt{group_name}
  - Specifies the name of secondary GTPP server group that is used as an alternate for the primary GTPP group associated with a specific APN for storage of GTPP messages. \texttt{group_name} must be an alphanumeric string of 1 through 63 characters. It must be the same name as configured earlier within the same APN context.

- \texttt{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 a specific APN.
actt_ctxt_name specifies the name of the context to be used for accounting as an alphanumeric string of 1 through 79 characters that is case sensitive.

Note that if an accounting context is not specified here, the system uses the GGSN service context or the context configured by the accounting context command in the GGSN Service Configuration mode.

Usage Guidelines

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 also be mirrored to the secondary servers.

This secondary group configuration is ignored, if the configured group_name is the same as the primary group. It will also be ignored, if the configured GTPP group_name and/or accounting context ac_context_name is invalid. In such cases, the call will be established successfully (unlike the primary group configuration where the call drops).

In the absence of a configured ac_context_name context, the GGSN service context is chosen by default.

The secondary group messages are low priority and thus are purged when there is no room for the new messages.

For more information on GTPP group, refer the description of the gtpp group command.

Examples

The following command applies a previously configured GTPP server group named star2 to a 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

Configures a session idle-timeout to be reset with uplink packets only, or with both uplink and downlink packets.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:
(context_name)host_name(config-apn)#

**Syntax Description**

idle-timeout-activity

idle-timeout-activity ignore-downlink

default idle-timeout-activity

default

Sets or restores the command to the default setting.

ignore-downlink

Sets the system to ignore the downlink traffic for consideration as activity for idle-timeout.

**Usage Guidelines**

If idle-timeout-activity ignore-downlink is configured, the downlink (network to subscriber) traffic will not be used to reset the idle-timeout. Only uplink (subscriber to network) 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.

**Examples**
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
ignore-alt-config

Configures preference to APN/AAA-defined behavior/parameters. If the parameters are not defined in APN/AAA, they will not be provisioned from any other source/configuration in the system, even if they are available there.

**Product**

- P-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**

```
[ no ] ignore-alt-config { no-dns | no-s6b }
```

- **no**
  
  Disables DNS server address preference or S6b authentication on a per-APN level.

- **no-dns**
  
  Gives preference to DNS server address configured in APN. If name server addresses is not found in APN configuration, it will not be provisioned from SGi context, even if it is configured there.

- **no-s6b**
  
  Enables/disables S6b authentication on a per-APN level.

  Ignores alternate service-level configuration for S6b authorization when S6b authorization is disabled at APN.

**Usage Guidelines**

Use this command to enable/disable DNS server address preference or S6b authentication on a per-APN level.

**Important**

Configuration in APN will take precedence over configuration in P-GW service configuration.
Examples

The following command to give preference to DNS server address configured in APN:

```bash
ignore-alt-config no-dns
```
ikev2 tsr

Configures the Traffic Selector responder (TSr) negotiation behavior during IKEv2 Security Association (SA) establishment.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax Description
{ default | ikev2 tsr { wildcard | user-specified } }

default
Specifies the default behavior, which is wildcard TSr negotiation.

wildcard
Specifies that during TSr negotiation, the PDG/TTG always returns an any-to-any IP address range, an any-to-any port range, and allows any protocol, irrespective of the traffic selector ranges received from the UE. This is the default behavior.

user-specified
Specifies that during TSr negotiation, the PDG/TTG responds to each UE request with the UE-specified IP address ranges. This enables split tunneling on the PDG/TTG, and enables the UE to tunnel only a specified traffic range to the PDG/TTG and send other traffic directly out the WLAN.

Usage Guidelines
Use this command to specify the TSr negotiation behavior on the PDG/TTG.

Examples
The following command enables user-specified TSr negotiation on the PDG/TTG:
ikev2 tsr user-specified
**ims-auth-service**

Applies an IMS (IP Multimedia Subsystem) authorization service to a subscriber through APN for Gx interface support and functionality.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

\[(context_name)host_name(config-apn)\#\]

**Syntax Description**
- `no ims-auth-service auth_service_name`

  **no**
  
  Disables the applied IMS authorization service for a specific APN.

  **auth_service_name**
  
  Specifies the name of the IMS authorization service name that is used for Gx interface authentication for a specific APN. `auth_service_name` must be a alphanumeric string of 1 through 63 characters preconfigured within the same context as this APN.

**Usage Guidelines**
This feature provides the IMS authorization service configuration for Gx interface in IMS service node.

**Examples**

The following command applies a previously configured IMS authorization service named `gx_interface1` to an APN within the specific context:

\[ims-auth-service gx_interface1\]

The following command disables the applied IMS authorization service `gx_interface1` for the specific APN:

\[no ims-auth-service gx_interface1\]
ip access-group

Configures an IPv4/IPv6 access group for the current APN profile.

**Product**
ACS
eWAG
GGSN
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

```plaintext
configure > context context_name > apn apn_name
```
Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**

```plaintext
ip access-group acl_group_name [ in | out ] [ fallback-enabled ]
[ 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 previously configured ACL group expressed as an alphanumeric 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.

- **fallback-enabled**
  When invalid ACL is received from RADIUS during Context Activation, ACL in this APN will be applied so there is no loss of CDR or missing charging information.
  By default, ACL fallback is disabled.
**Usage Guidelines**

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 is specified, the selected access control list will be applied to both directions.

Run command without **fallback-enabled** option to disable ACL fallback for a previously configured ACL applied to a particular APN.

**Examples**

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 command 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
SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-apn)#
```

**Syntax Description**

```
ip address alloc-method { dhcp-proxy [ allow-deferred ] [ prefer-dhcp-options ] | dhcp-relay | local [ allow-deferred ] | no-dynamic [ allow-deferred ] | allow-user-specified }
default ip address allocation-method
```

**default**

Restores the APN ip parameters to the following default settings.

**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**

Configures the APN to forward DHCP packets received from the MS to a DHCP server. Default: Disabled

---

**Important**

If this option is used, the system's DHCP parameters must be configured.
local
Configures the APN to allocate IP addresses from a pool configured in the destination context on the system.
Default: Enabled

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
Disables the dynamic assignment of IP addresses to PDP contexts using this APN. Default: Disabled
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
If this keyword is specified with `dhcp-proxy` for IP address allocation configuration, the GGSN will prefer DHCP-supplied parameters over values provided by AAA server or by local configuration. This keyword controls the following parameters:
- primary and secondary Domain Name Server (DNS) addresses
- primary and secondary NetBIOS Name Server (NBNS) addresses

These values will be sent out in the PCO IE of a GTP Create PDP Response Message whenever the MS Requests them in A Create PDP Request Message.
Default: Disabled

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 received from a DHCP server will not be considered by the GGSN.

allow-defered
Enables support for P-GW deferred address allocation. Default: Disabled

allow-user-specified
Enables support for PDP contexts requesting the use of specific (static) addresses. Default: Enabled

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 Guidelines
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. The figure in the Example section below displays the process used by the system to determine how the address should be allocated.

**Examples**

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 3: IP Address Allocation Process*
ip address pool

Configures the name of an IP address pool configured on the system from which to assign an address for a PDP context.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

\[(context_name)|host_name|\(config-apn)\#

Syntax Description

{ no } ip address pool name pool_name

no

Removes a previously configured pool name.

pool_name

Specifies the name of the pool configured on the system from which an IP address will be assigned. The name is expressed as an alphanumeric string of 1 through 31 characters that is case sensitive.

Usage Guidelines

If the ip address alloc-method command is configured to allow the assignment of IP addresses from a local pool configured on the system. It command instructs the system as to which pool should be used.

The pool specified by this command must be a pool configured in the destination context on the system. Please refer to the ip pool command in the Context Configuration Mode Commands chapter 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.
From 14.0 onward for configuration of multiple IP pool in an APN, GGSN expects Framed-IP-Address and Framed-Pool from RADIUS.

Caution

In pre-release 14.0, the maximum number of IP pools in an APN is 16 for static and dynamic type of pool. From 14.0 onward this limit has been changed for static address allocation to 1 and out of the maximum 16 pools which can be configured under a particular APN, the first IP pool should be a static pool, which is the only working static pool from an APN.

Examples

The following command configures the system to use a pool named *private_pool1* for address allocation:

```
ip address pool private_pool1
```
**ip address pool-exhaust-action**

Configures the behavior to accept/reject a call if the IPv4 address pool is exhausted.

**Product**

- GGSN
- P-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-apn)#
```

**Syntax Description**

```
ip address pool-exhaust-action { ipv6-accept | ipv6-reject }
```

- **ipv6-accept**
  GGSN/P-GW will not reject the call; follows the standard behavior of allocating the available IP address.

- **ipv6-reject**
  Enables rejecting a call if GGSN/P-GW cannot allocate the IPv4 address for PDN type IPv4v6.

**Usage Guidelines**

As per the standard behavior, when a UE sends a Create Request to GGSN/P-GW with PDN type IPv4v6, it should allocate both IPv4 and IPv6 address to the UE. If GGSN/P-GW fails to allocate the IPv4 address due to IP pool exhaustion, then it allocates only IPv6 address and changes the PDN Type to IPv6 and the call continues. In order to control this behavior, this CLI has been introduced; when configured, the following behavioral scenarios will be in place:

- CLI executed with **ipv6-reject** option will reject a call if GGSN/P-GW cannot allocate the IPv4 address for PDN type IPv4v6.
- CLI executed with **ipv6-accept** option will not reject a call and follow the standard behavior.

**Examples**

The following command will reject a call if IPv4 type address allocation is not possible by GGSN/P-GW:

```
ip address pool-exhaust-action ipv6-reject
```
**ip context-name**

Configures the name of the destination context to use for subscribers accessing this APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
  ```
  configure > context context_name > apn apn_name
  ```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**

```
[ no ] ip context-name ctxt_name
```

- **no**
  Removes a previously configured context name.

- **ctxt_name**
  Specifies the name of the context through which subscriber data traffic will be routed. `ctxt_name` must be an alphanumeric string from 1 to 79 characters.

**Usage Guidelines**

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 (foreign Agent) service is configured. If no name is specified, the context in which the GGSN service facilitating the subscriber PDP context is used.

**Examples**

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
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

```bash
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-apn)#
```

**Syntax Description**
- `ip header-compression vj`
- `default ip header-compression`
- `no ip header-compression`

- **default**
  Disables Van-Jacobson header compression.

- **no**
  Disables Van-Jacobson header compression.

- **vj**
  Enables Van-Jacobson header compression for IP packets. Default: Enabled

**Usage Guidelines**
IP header compression reduces packet header overhead resulting in more efficient utilization of available bandwidth.

**Examples**
The following command disables packet header compression for the APN:

```
no ip header-compression
```
ip hide-service-address

Renders the IP address of the GGSN unreachable from mobile stations (MSs) using this APN. This command is configured on a per-APN basis.

Product
- GGSN
- P-GW
- SAEGW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > APN Configuration
```
configure > context context_name > apn apn_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-apn)#
```

Syntax Description
```
[ default | no ] ip hide-service-address
```
- **default**
  Does not allow the mobile station to reach the GGSN IP address using this APN.
- **no**
  Allows the mobile station to reach the GGSN IP address using this APN.

Usage Guidelines
This hides the GGSN IP address from the mobile station for security purposes.

Examples
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
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-apn)#
```

**Syntax Description**
- **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 IPv4 dotted-decimal notation.

**Usage Guidelines**

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.

**Examples**

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
- SAEGW

Privilege
- Security Administrator
- Administrator

Command Modes
- Exec
- Global Configuration
- Context Configuration
- APN Configuration

configure > context context_name > apn apn_name

Syntax Description

[ default | no ] ip multicast discard

default
Restores the APN IP parameters to the default multicast settings, which is to discard PDUs.

no
Removes a previously configured IP multicast discard.

Usage Guidelines
This command specifies if IP multicast discard is enabled or disabled.

Examples
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 of a particular 3GPP QoS class over the Gi interface.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

<context_name>host_name(config-apn)#

Syntax Description

ip qos-dscp { qci { 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 } { dscp } } +
default ip qos-dscp

no ip qos-dscp { qci { 1 | 2 | 3 | 4 | 5 } allocation-retention-priority { 1..3 } } | 6 { allocation-retention-priority { 1..3 } } | 7 { allocation-retention-priority { 1..3 } } | 8 { allocation-retention-priority { 1..3 } } | 9 } } +
default

Restores the APN IP parameters to the default setting conversational ef streaming af11 interactive af21 background be.

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 17: 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></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>ef</td>
<td>ef</td>
<td>ef</td>
</tr>
<tr>
<td>3</td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
<tr>
<td>4</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.

### qci

Configures the QoS Class Identifier (QCI) attribute of QoS. Here the `qci_val` is the QCI for which the negotiate limit is being set; it ranges from 1 to 9.

### dscp

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
- `pt`: Pass through (ToS of user packet is not modified)
• **af32**: Assured Forwarding 32 PHB

Default: QCI:
- 1: ef
- 2: ef
- 3: af11
- 4: af11
- 5: ef
- 6: ef
- 7: af21
- 8: af21
- 9: be

More than one of the above keywords can be entered within a single command.

**Usage Guidelines**

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 traffic patterns are defined by QCI (1 to 9). 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 18: 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>
</tbody>
</table>
### Precedence (low to high) vs DSCP

<table>
<thead>
<tr>
<th>Precedence (low to high)</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<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.

---

**Important**

If a GGSN service is associated with a P-GW service, then the GGSN service will use the QCI-QoS mapping tables specified in the `qci-qos-mapping` command and assigned to its associated P-GW service.

---

**Examples**

The following command configures the DSCP level for QCI to be Expedited Forwarding, ef:

```
ip qos-dscp qci 1 ef
```
**ip source-violation**

Enables or disables packet source validation for the current APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- ```configure > context context_name > apn apn_name```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**
```
ip source-violation { ignore | check [ drop-limit limit ] [ exclude-from-accounting ] }
default ip source-violation
```

**default**

Enables the checking of source addresses received from subscribers for violations, with a drop limit of 10 invalid packets that can be received from a subscriber prior to their session being deleted.

**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 statistics generated for accounting records.

Usage Guidelines
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.

Examples
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

Controls the copying of the IP ToS octet value from user IPv4/IPv6 datagrams into the IP header of GTP tunnel encapsulations.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[(context_name)host_name](config-apn)#

Syntax Description

[ default | no ] ip user-datagram-tos copy

default
Sets the default behavior of this command. By default this function is disabled.

no
Removes the preconfigured parameter for this command.

Usage Guidelines

This command enables or disables the copying of the ToS byte from the inner IP header to the outer IP header for an RP connection.

When this function is enabled, the SGSN can detect the special ToS marking in the outer IP header of GTP tunnel packets and identify certain packets as control messages.
ipv6 access-group

Configures the IPv6 access group for the current APN profile which applies a single Access Control List (ACL) to multiple subscribers via the APN for IPv6 traffic.

**Product**
- GGSN
- ACS
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-apn)#`

**Syntax Description**

`ipv6 access-group group_name [ in | out ] | fallback-enabled ]`

`[ no | ipv6 access-group group_name [ in | out ]`

**no**

Removes a previously configured IPv6 ACL applied to a particular APN for IPv6 traffic. If at least one of the two `{ in | out }` options is not selected for the ACL that will be removed, the ACL will be removed for both directions.

**group_name**

Specifies the name of the IPv6 access group as an alphanumeric string of 1 through 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 no direction is supplied in the base command, the specified IPv6 access control list will be applied to both directions.
**fallback-enabled**

When invalid ACL is received from RADIUS during Context Activation, ACL in this APN will be applied so there is no loss of CDR or missing charging information.

By default, ACL fallback is disabled.

**Usage Guidelines**

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 is specified, the selected access control list will be applied to both traffic directions.

Run command without **fallback-enabled** option to disable ACL fallback for a previously configured ACL applied to a particular APN.

**Examples**

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 alloc-method

Controls the IPv6 address allocation method for a particular APN.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration
```
configure > context context_name > apn apn_name
```

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

**Syntax Description**

ipv6 address alloc-method \{ dhcpv6-proxy [allow-prefix-delegation] | local | no-dynamic \} \{ allow-user-specified \} \{ default \} ipv6 address alloc-method

**default**

Configures the default address allocation method which is "local".

**dhcpv6-proxy**

Configures the IPv6 address from DHCP server for the APN.

**allow-prefix-delegation**

Configures the APN to allow DHCPv6 prefix-delegation.

**local**

Configures the IPv6 address from the local pool configured.

**no-dynamic**

Configures the IPv6 address as indicated by the authentication server.

**allow-user-specified**

When any of the above three options is specified with **allow-user-specified**, the static IP address provided by UE takes priority and allocated/configured.
**Usage Guidelines**

With the support of DHCPv6 and dual PDP IPv4v6, the separate allocation methods are required for IPv4 and IPv6. Earlier the IPv6 address was allocated through locap pool or RADIUS Returned, but with the new options: local, no-dynamic, and DHCPv6-proxy, the IPv6 address allocation can be done for a particular APN. The static address allocation can be enabled by the use of `allow-user-specified` keyword with the above three options.

From 15.0 onward the support of prefix delegation for DHCPv6 is added to assign a network address prefix to a user site, configuring the user's router with the prefix to be used for each interface it is attached to. This is one of the methods for delegating IPv6 address prefixes to an IPv6 subscriber's network.

**Examples**

The following command provides an example of allocating the IP address from DHCP server:

```
ipv6 address alloc-method dhcpv6-proxy allow-user-specified
```

The following commands configure the prefix-delegation for DHCPv6 with 52 bit length:

```
ipv6 address alloc-method dhcpv6-proxy allow-prefix-delegation
ipv6 address prefix-delegation-len 52
```
ipv6 address delegate-prefix-pool

Configures the private pool name to be used for delegate prefix allocation.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

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

Syntax Description

ipv6 address delegate-prefix-pool pool_name
[ no ] ipv6 address delegate-prefix-pool

delegate-prefix-pool:
Configures a pool of IPv6 address delegated prefix.

pool_name:
Name of the pool with IPv6 address delegated prefix.

no
Disables the pool of IPv6 address delegated prefix.

Usage Guidelines

With this command, configure the IPv6 private pool name to enable the prefix delegation from the local pool.

Examples

The following command provides an example of creating a pool of IPv6 address delegated prefix:
ipv6 address delegate-prefix-pool pool1
**ipv6 address prefix-delegation-len**

Configures the supported prefix length to 48/52/56 bit length per-APN for DHCPv6 prefix-delegation support.

**Syntax Description**

```plaintext
| no | ipv6 address prefix-delegation-len {48 | 52 | 56}
```

- `no`

Removes the configured prefix-delegation length to allow DHCPv6 prefix delegation.

**Usage Guidelines**

Use this command to configure the length of prefix (48/52/56) to allow with DHCPv6 prefix delegation.

**Examples**

The following command sets the allowed prefix length to 52 bit for DHCPv6 prefix delegation support:

```plaintext
ipv6 address prefix-delegation-len 52
```
ipv6 address pool-exhaust-action

Configures the behavior to accept/reject a call if the IPv6 address pool is exhausted.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-apn)#
```

**Syntax Description**

```
ipv6 address pool-exhaust-action { ipv4-accept | ipv4-reject }
```

**ipv4-accept**
- GGSN/P-GW will not reject the call; follows the standard behavior of allocating the available IP address.

**ipv4-reject**
- Enables rejecting a call if GGSN/P-GW cannot allocate the IPv6 address for PDN type IPv4v6.

**Usage Guidelines**

As per the standard behavior, when a UE sends a Create Request to GGSN/P-GW with PDN type IPv4v6, it should allocate both IPv4 and IPv6 address to the UE. If GGSN/P-GW fails to allocate the IPv6 address due to IP pool exhaustion, then it allocates only IPv4 address and changes the PDN Type to IPv4 and the call continues. In order to control this behavior, this CLI has been introduced; when configured, the following behavioral scenarios will be in place:

- CLI executed with **ipv4-reject** option will reject a call if GGSN/P-GW cannot allocate the IPv6 address for PDN type IPv4v6.
- CLI executed with **ipv4-accept** option will not reject a call and follow the standard behavior.

**Examples**

The following command will reject a call if IPv6 type address allocation is not possible by GGSN/P-GW:

```
ipv6 address pool-exhaust-action ipv4-reject
```
ipv6 dns

Configures primary and secondary IPv6 Domain Name Service (DNS) servers.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

`{context_name}host_name(config-apn)#`

**Syntax Description**
```
[ no ] ipv6 dns { primary | secondary } { ipv6_dns_address }
```

- **no**
  Deletes a previously configured DNS server.

- **primary**
  Configures the IPv6 address of primary DNS server for the APN.

- **secondary**
  Configures IPv6 address of the secondary DNS server for the APN. Only one secondary DNS server can be configured.

- **ipv6_dns_address**
  The IP address of the DNS server entered using IPv6 colon-separated-hexadecimal notation.

**Usage Guidelines**
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 (NetBIOS Name Service) servers to be negotiated via ICPC (Initial Connection Protocol Control) with the LNS (L2TP Network Server). |

| Examples | The following command provides an example of setting the primary DNS server: `ipv6 dns primary fe80::c0a8:a04` |
ipv6 egress-address-filtering

Enables or disable IPv6 egress address filtering. This function 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 node. When packets sent to the mobile node are received, the destination interface ID is compared against the list of recorded interface IDs and with the local interface-ID assigned to the MS during IPv6CP. If no match is found, the packet is dropped.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-apn) #

Syntax Description

[ no ] ipv6 egress-address-filtering

no

Disables IPv6 egress address filtering.

Usage Guidelines

Used to filter packets that arrive from the internet to a particular site.

Examples

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  
SAEGW

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > APN Configuration  
```
configure > context context_name > apn apn_name
```
Entering the above command sequence results in the following prompt:  
```
[context_name]host_name(config-apn)>
```

**Syntax Description**

```
ipv6 initial-router-advt { interval int_value | num-advts num_value | option mtu }
[ default ] ipv6 initial-router-advt { interval | num-advts| option mtu }
no ipv6 initial-router-advt option mtu
```

**default**  
Resets interval or num-advts to their default setting.

**interval int_value**  
Specifies the time interval (in milliseconds) when the initial IPv6 router advertisement is sent to the mobile node as an integer from 100 through 16000. Default: 3000ms

**num-advts value num_value**  
Specifies the number of initial IPv6 router advertisements sent to the mobile node as an integer from 1 through 16. Default: 3

**Usage Guidelines**  
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.
**option mtu**

Enables the gateway to send the IPv6 MTU option in RAs for IPv6 and IPv4v6 PDN types towards the UE. As a result, the UE can send uplink data packets based on the configured MTU and perform fragmentation at the source, if required.

The default setting is enabled.

The `no` keyword disables this feature. The IPv6 MTU option in RAs for IPv6 and IPv4v6 PDN types will not be sent towards the UE.

**Examples**

The following command specifies the initial ipv6 router interval to be 2000ms:

```
ipv6 initial-router-advt interval 2000
```
**l3-to-l2-tunnel address-policy**

Configures the address allocation/validation policy, when subscriber L3 (IPv4/IPv6) sessions are tunneled using an L2 tunneling protocol, such as L2TP.

**Product**

GGSN

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**

```
l3-to-l2-tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }
default l3-to-l2-tunnel address-policy
```

**default**

Restores the layer 3-to-layer 2 tunnel address policy parameter to the default setting of validation with no allocation.

**alloc-only**

Specifies that the system locally allocates and validates subscriber addresses. Default: Disabled

**alloc-validate**

Specifies that the system allocates addresses when IP addresses are dynamically assigned. The system does not validate the address specified by the subscriber. Default: Disabled

**no-alloc-validate**

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. Default: Enabled
Usage Guidelines
This command can be useful for MIP HA sessions tunneled from the system using L2TP tunnels, or GGSN PDP contexts of type IP tunneled using L2TP to a remote LNS.

Examples
The following command configures the system to locally allocate and validate subscriber addresses:
l3-to-l2-tunnel address-policy alloc-only
loadbalance-tunnel-peers

Configures how tunnel-peers are selected for this APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration

    configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

    {context_name}host_name(config-apn)#

**Syntax Description**
- loadbalance-tunnel-peers { balanced | prioritized | random }
- default loadbalance-tunnel-peers

- **default**
  Restores the loadbalance-tunnel-peers parameter to the default setting of random.

- **balanced**
  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. Default: Disabled

- **prioritized**
  Tunnel-peer selection is made based on the priority configured for the peer. Default: Disabled

- **random**
  Tunnel-peer selection is random in order. Default: Enabled

**Usage Guidelines**
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.
Examples

The following command sets the APN to connect to tunnel-peers in a sequential order:

```
load-balancing balanced
```
## long-duration-action detection

Sets the detection of a session that exceeds the long duration timer and sends notification.

### Product
All

### Privilege
Security Administrator, Administrator

### Command Modes
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name (config-apn) #
```

### Syntax Description
- `long-duration-action detection`
- `default long-duration-action`

#### default
Restores the long-duration-action parameter to its default setting of detection.

- `long-duration-action detection`

Detects long duration sessions and sends SNMP TRAP and CORBA notification. This is the default behavior. Default: Enabled

### Usage Guidelines
Use this command to detect a session that exceeds the limit set by the long duration timer.

Refer to the `timeout idle` and `timeout long-duration` commands for information on setting the long duration timer.

### Examples
Use the following command to enable detecting the session that exceeds the long duration timer:

`long-duration-action detection`
long-duration-action disconnection

Specifies what action is taken when the long duration timer expires.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context  context_name > apn  apn_name
```

Entering the above command sequence results in the following prompt:
```
(context_name)host_name(config-apn)#
```

**Syntax Description**

```
long-duration-action disconnection  [ suppress-notification ] [ dormant-only ] +
```

- **long-duration-action disconnection**
  Detects a long duration session and disconnects the session after sending SNMP TRAP and CORBA notification. Default: Disabled

- **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. It sends the SNMP TRAP and CORBA notification after disconnecting a long duration session. Default: Disabled

**Usage Guidelines**
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.

**Examples**
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`
**mbms bmsc-profile**

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
- SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-apn) #
```

**Syntax Description**

```
mbms bmsc-profile name bmsc_profile_name
| default | no | mbms bmsc-profile
```

**default**

Applies the default BMSC profile to the subscribers through the APN.

**no**

Deletes a previously associated BM-SC profile with this APN.

**name bmsc_profile_name**

Specifies a name for the BM-SC profile already configured in BMSC configuration mode. `bmsc_profile_name` is an alphanumeric string of 1 through 79 characters that may contain dots (.) and/or dashes (-).

**Usage Guidelines**

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 to the **BMSC Profile Configuration Mode Commands** chapter.

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.
Examples

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 Multimedia Broadcast Multicast Service (MBMS) bearer contexts with this MBMS APN.

Product

- GGSN
- P-GW
- SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-apn)#

Syntax Description

mbms bearer timeout { absolute | idle } time
| default | no | mbms bearer timeout { absolute | idle }

default

Sets the default value for the followed option for MBMS bearer context timeout.

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.

absolute

Configures the absolute maximum time (in seconds) an MBMS bearer context may exist in any state (active or idle). Default: Disabled

idle

Default: Disabled

Configures the maximum amount of time (in seconds) an MBMS bearer context may be idle.
**mbms bearer timeout**

*time*

*time* can be any integer value between 0 and 4294967295. A time of 0 disables timeouts for this APN. Default: 0

**Usage Guidelines**

Use this command to limit the amount of time that an MBMS bearer context session can remain connected.

**Examples**

The following commands enables an absolute time timeout of 60000 seconds for MBMS bearer context:

```plaintext
mbms bearer timeout absolute 60000
```
mbms ue timeout

Configures the session timeout values for the Multimedia Broadcast Multicast Service (MBMS) user equipment (UE) contexts with this MBMS APN.

Product
- GGSN
- P-GW
- SAEGW

Privilege
- Security Administrator
- Administrator

Command Modes
`Exec > Global Configuration > Context Configuration > APN Configuration`

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

Syntax Description
```
mbms ue timeout absolute time
[ default | no ] mbms ue timeout absolute

default
Set the default value for the followed option for MBMS UE context timeout.

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.

absolute time
Configures the absolute maximum time (in seconds) an MBMS UE context may exist in any state (active or idle). `time` can be any integer value between 0 and 4294967295. A time of 0 disables timeouts for this APN. Default: 0
```

Usage Guidelines
Use this command to limit the amount of time that an MBMS UE context session can remain connected.

Examples
The following commands enables an absolute time timeout of 60000 seconds for MBMS UE context:
```
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
- SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

Syntax Description

```
mediation-device [ context-name context_name ] [ delay-GTP-response ] [ no-early-PDUs ] [ no interims ] [ default | no ] mediation-device
```

+ Indicates that more than one of the options can be specified with a single execution of the command.

**default**

Changes the mediation device to no context-name configured and restores the mediation device's default properties.

**no**

Deletes the mediation-device configuration.

**context-name context_name**

Configures the mediation VPN context for this APN as an alphanumeric string of 1 through 79 characters that is case sensitive. If not specified, the mediation context is the same as the destination context of the subscriber. Default: The subscriber's destination context.
delay-GTP-response
When enabled, delays the CPC response until an Accounting Start response is received from the mediation device. Default: Disabled

no-early-pdus
Specifies that the system delays PDUs from the MS until a response to the GGSN accounting start request is received from the mediation device. The PDUs are queued, not discarded. Default: Disabled

If "no-early-PDUs" is enabled, the chassis does not send uplink/downlink data from/to a MS until it receives the Acct-Rsp Start for the same from the mediation device. On receiving the Acct-Rsp, pending PDUs are forwarded. The chassis buffers up to two PDUs per call. As soon as the third PDU comes, the buffering is disabled and all the PDUs are forwarded for that call.

Configures the system to queue up to two PDUs until the mediation device returns a response to the system's accounting START request per 3GPP standards. On receiving the Accounting response message, the system forwards the subsequent PDUs without discarding any of the packets.

Important
For StarOS 10.0 and earlier releases, the system buffers up to four PDUs and queues or discards the remaining PDUs.

Important
For StarOS 11.0 and later releases, the system is configured so that none of the PDUs are discarded.

no-interims
Disables sending interims to the mediation server. Default: Disabled

Important
Different commands are used to disable RADIUS interims for RADIUS accounting and mediation accounting. To disable RADIUS interims for mediation accounting, use the following command: mediation-device context-name context_name no-interims. To disable RADIUS interims for RADIUS accounting, use the following command: accounting-mode radius-diameter no-interims.

Usage Guidelines
This command enables 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.

Examples
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
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-apn)#
```

**Syntax Description**
- `mobile-ip home-agent ip_address [ alternate ]`
- `no mobile-ip home-agent ip_address alternate`
- `default mobile-ip home-agent`

**Default**
Restores the APN mobile-ip parameters to the default setting, no HA address defined.

**No**
Removes a previously configured HA address.

**ip_address**
Specifies the IP address of the HA expressed in IPv4 dotted-decimal notation.

**alternate**
Designates this Mobile IP HA as the alternate that will be used in the event of a fail-over.

**Usage Guidelines**
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.
Examples

The following command configures an HA IP address of 192.168.1.15:

```
mobile-ip home-agent 192.168.1.15
```
mobile-ip min-reg-lifetime-override

Specifies the minimum registration timer to override the platform-wide default on an enterprise basis. This feature is associated with 4G LTE scenarios employing Network Mobility (NEMO) routing.

**Product**
- P-GW
- HA

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-apn)#
```

**Syntax Description**
- `mobile-ip min-reg-lifetime-override { seconds | infinite }
- default mobile-ip min-reg-lifetime-override
- no mobile-ip min-reg-lifetime-override`

**default**
Sets the minimum registration time to 600 seconds.

**no**
Deletes the registration interval entered via this command.

**seconds**
Specifies the minimum registration interval in seconds as an integer from 1 through 65534. Default = 600

**infinite**
Sets the minimum registration interval as "infinite" (forever) for this subscriber.

**Usage Guidelines**
Specify the minimum registration timer to override the platform-wide default on an enterprise basis. With this command, NEMO traffic could be re-routed symmetrically to an alternate carrier within the specified number of seconds following a failure on the primary communication path.
Examples

The following command sets the minimum registration override interval to 900 seconds:

```
mobile-ip min-reg-reg-lifetime-override 900
```
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
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
<context_name>host_name>(config-apn)#
```

**Syntax Description**

- `| default | no | mobile-ip mn-aaa-removal-indication`

  **default**
  
  Sets the default setting for mobile IP MN-AAA-Removal-Indication.

  **no**
  
  Disables this functionality. This is the default setting.

**Usage Guidelines**

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.
mobile-ip mn-ha-hash-algorithm

Designates the encryption algorithm to use for Hash-based Message Authentication Code (HMAC).

**Product**

GGSN  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```plaintext
<context_name> host_name (config-apn) #
```

**Syntax Description**

mobile-ip mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }

default mobile-ip mn-ha-hash-algorithm

default

Designates the default encryption algorithm to use.

hmac-md5 | md5 | rfc2002-md5

Default: hmac-md5

The encryption algorithms that may be used.

**Usage Guidelines**

Provides security by encrypting the data.

**Examples**

The following command sets encryption for md5:

```plaintext
mobile-ip mn-ha-hash-algorithm md5
```
**mobile-ip mn-ha-shared-key**

Configures the subscriber MobileNode-Home Agent (MN-HA) shared key.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration
`configure > context context_name > apn apn_name`
Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-apn)#
```

**Syntax Description**
- `mobile-ip mn-ha-shared-key key`
- `no mobile-ip mn-ha-shared-key`

- `no`
  Disables this functionality. This is the default setting.

- `key`
  Specifies the subscriber MN-HA shared key as either an alphanumeric string or a hexadecimal number sequence beginning with "0x". The string or sequence consists of 16 to 127 characters.

**Usage Guidelines**
Configures a shared key for the APN.

**Examples**
The following command configures a shared key as the alphanumeric string `sfd23408imi9yn`:
```
mobile-ip mn-ha-shared-key sfd23408imi9yn
```
mobile-ip mn-ha-spi

Configures the Mobile IP Security Parameter Index (SPI).

**Product**
GGSN  
P-GW  
SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-apn)#
```

**Syntax Description**
- `mobile-ip mn-ha-spi spi_number`
- `no mobile-ip mn-ha-spi`

**no**
Disables this functionality. This is the default setting.

**spi_number**
Specifies the SPI as an integer from 256 through 4294967295.

**Usage Guidelines**
Configures an SPI for the APN.

**Examples**
The following command configures an SPI of 15111111111111111111111111111111:

```
mobile-ip mn-ha-spi 15111111111111111111111111111111
```
mobile-ip required

Enables support for Mobile IP functionality for all PDP contexts facilitated by the current APN.

Product

- GGSN
- FA
- P-GW
- SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-apn)#
```

Syntax Description

```
| default | no | mobile-ip required
```

- **default**
  
  Applies the default setting for mobile-ip for the APN. Default is disabled.

- **no**
  
  Disables mobile-ip for the APN.

Usage Guidelines

Mobile IP functionality for IP PDP contexts is only supported at the APN-level. This command enables or 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.
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
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**

```
[ default | no ] mobile-ip reverse-tunnel
```

**default**
Designates the default reverse tunnel for the APN. The default is enabled.

**no**
Disables this functionality.

**Usage Guidelines**
Use this command to enable support for Mobile IP reverse tunneling for the APN. Reverse tunneling is enabled by default.
nai-construction

Configures the Network Access Identifier (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
SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:
(context_name)host_name(config-apn)##

Syntax Description

nai-construction { imsi | msisdn } [override-null-username] [encrypted password encrypt_password | use-shared-secret-password | password password ]
nono nai-construction

no
Disables the NAI construction at the APN level.

imsi
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. Default: Enabled

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 an alphanumeric string of 0 through 63 characters.

**password**
Configures the authentication user-password for this NAI-constructed user. *password* is an alphanumeric string of 0 through 63 characters.

**use-shared-secret-password**
Specifies use of the RADIUS authentication shared secret password for this NAI-constructed user.

**Usage Guidelines**
NAI-construction defines the behavior for construction at the APN level. If defined for a particular APN, this command 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 the **aaa nai-construction authentication** command in Context Configuration Mode.

**Examples**
The following command enables NAI-construction using IMSI as the authentication type with an encrypted password:
```
nai-construction imsi encrypted password s1289sf980333jwwdo97342
```
nbns

Configures and enables use of NetBios Name Service (NBNS) for the APN.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

{context_name|host_name}(config-apn)#

Syntax Description

| 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 an IPv4 address in dotted-decimal notation.

secondary

Designates secondary/failover NBNS server. Must be followed with an IPv4 address in dotted-decimal notation.

IP_address

Specifies the IP address in IPv4 dotted-decimal notation.

Usage Guidelines

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.
Examples

The following command configures the APN's NetBios Name Service to primary IP 192.168.1.15.

nbns primary 192.168.1.15
network-behind-mobile

Allows enabling/disabling the Network Behind Mobile Station (NBMS) for the APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
```
Exec > Global Configuration > Context Configuration > APN Configuration
``` configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:
```
{context_name}@host_name(config-apn)>
```

**Syntax Description**

```
network-behind-mobile { max-addresses-behind-mobile max_addrs | max-subnets max_subnets } | default | no | network-behind-mobile
```

**default**

Enables the default settings for this function. It enables NBMS with max-subnets as 10 and max-addresses-behind-mobile as 16,777,214 default values.

**no**

Disables the network behind mobile station functionality on the APN.

**max-addresses-behind-mobile max_addrs**

Configures the maximum number of addresses that are allowed in a single Network/subnet Behind MS.

`max_addrs` must be an integer from 1 through 16,777,214.

Default: 16,777,214

**max-subnets max_subnets**

Specifies the maximum number of subnets that can be enabled for a call in the APN.

`max_subnets` must be an integer from 1 through 16.

Default: 10
Usage Guidelines

Use this command to enable or disable NBMS for the APN.

Examples

The following command enables NBMS and allows a maximum of 16 routes to be installed on the APN wherein maximum 268,435,454 host addresses are allowed in each network:

```
network-behind-mobile max-subnets 16
```
**nexthop-forwarding-address**

Configures the next hop forwarding address for the APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-apn)>
```

**Syntax Description**
- **nexthop-forwarding-address ipv4_address**
- **no nexthop-forwarding-address**

  **no**
  
  Disables this function. This is the default setting.

  **ipv4_address**
  
  Specifies the next hop forwarding address for the APN. Must be an IPv4 address in dotted-decimal notation. Ensure the route is available for this next hop address and its directly connected host. Use of an arbitrary address can cause a routing loop within the host and lead to dropped packets.

**Usage Guidelines**
Use this command to configure the next hop forwarding address for the APN.

**Examples**

The following command configures the next hop forwarding address to 10.1.1.1:

```
nexthop-forwarding-address 10.1.1.1
```
npu qos

Configures an NPU QoS priority queue for packets facilitated by the APN.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

{context_name} host_name(config-apn) #

Syntax Description

npu qos traffic priority { best-effort | bronze | derive-from-packet-dscp | gold | silver }
default npu qos traffic priority

default

Configures the default NPU QoS traffic priority.

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: Specifies that the priority is to be determined from the DSCP (Differentiated Services Code Point) field in the packet's TOS octet. Default: Enabled
gold: Assigns the gold queue priority. This is the highest priority.
silver: Assigns the silver queue priority. This is the second-highest priority.

Usage Guidelines

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 Administration Guide* for additional information on NPU QoS functionality.

**Examples**

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.

### Product
- GGSN
- P-GW
- SAEGW

### Privilege
Security Administrator, Administrator

### Command Modes
```
Exec > Global Configuration > Context Configuration > APN Configuration
```
```
configure > context context_name > apn apn_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-apn)#
```

### Syntax Description
```
outbound { [ encrypted ] password pwd | username name }
no outbound password | username
```

**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 as an alphanumeric string of 1 through 132 characters that is case sensitive.

**username name**
Specifies the username to use for session authentication as an alphanumeric string of 1 to 127 characters that is case sensitive.
**Usage Guidelines**

This command can be used to provide a username and password for authentication when the subscriber does not 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.

**Examples**

The following commands configures an APN username of `isp1` and a password of `secRet123`.

```
outbound username isp1
outbound password secRet123
```
paging-policy-differentiation

Controls Paging Policy Differentiation (PPD) functionality on the P-GW.

**Product**
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**
```
[ default | no ] paging-policy-differentiation
```

- **default**
  Restores the PPD functionality to its default setting of disabled.

- **no**
  Disables this option. This is the default setting.

**Usage Guidelines**

To support PPD feature in SAEGW, both S-GW and P-GW configuration is required.

```
Usage Guidelines
Use this command to enable/disable PPD functionality on P-GW.
```
P-GW and S-GW should apply the PPD feature for both Default and Dedicated bearers. As per the specifications, P-GW transparently passes the user-datagram packet towards S-GW. This means, if PPD feature is enabled, operator can't apply different behavior for Default and Dedicated bearers.

Once the PPD feature is enabled, it is applicable for new calls.

For the PPD feature to work, it must be enabled for P-GW and S-GW.

Both P-GW and S-GW services apply PPD configuration independently. Therefore, for any downlink data packet from an APN, there could be a case where P-GW does not have PPD configuration but S-GW has PPD configuration. To avoid such a conflict, you must configure the PPD functionality on both P-GW (APN level granularity) and S-GW (service level granularity).

See the Paging Policy Differentiation chapter in the P-GW Administration Guide for detailed information on PPD functionality.

**Examples**

To enable PPD functionality on P-GW, enter the following command:

```
paging-policy-differentiation
```
**p-cscf**

Enables use of locally configured Proxy Call Session Control Function (P-CSCF) addresses or a Fully Qualified Domain Name (FQDN).

**Product**

P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn) #
```

**Syntax Description**

In StarOS V14.x and earlier:

```
p-cscf { fqdn fqdn | primary [ ip IPv4_address | IPv6 IPv6_address ] | secondary [ ip IPv4_address | IPv6 IPv6_address ] }
```

In StarOS V15.0 and later:

```
p-cscf { fqdn fqdn | priority address_priority [ ip IPv4_address | ipv6 IPv6_address ] }
no p-cscf { fqdn fqdn | priority address_priority [ ip | ipv6 ] }
```

**no**

Disables use of previously configured P-CSCF addresses or FQDN.

**fqdn fqdn**

Configures the P-CSCF FQDN server name for the APN as an alphanumeric string of 1 through 256 characters.

**primary [ ipIPv4_address | ipv6 IPv6_address ]**

Specifies the primary P-CSCF address for the APN.

*IPv4_address* must be expressed in IPv4 dotted-decimal notation.

*IPv6_address* must be expressed in IPv6 colon-separated-hexadecimal notation.
secondary [ ip IPv4_address | ipv6 IPv6_address ]

Specifies the secondary P-CSCF address for the APN.
IPv4_address must be expressed in IPv4 dotted-decimal notation.
IPv6_address must be expressed in IPv6 colon-separated-hexadecimal notation.

priority address_priority [ ip IPv4_address | ipv6 IPv6_address ]

Specifies the priority for P-CSCF address for the APN.
address_priority is an integer from 1 to 3. 1 is the highest priority.
IPv4_address must be expressed in IPv4 dotted-decimal notation.
IPv6_address must be expressed in IPv6 colon-separated-hexadecimal notation.

Usage Guidelines
Use this command to specify the P-CSCF addresses or FQDN server name associated with this APN.

Examples
The following command enables a P-CSCF with the primary IPv4 address 10.2.3.4 for the APN:
\texttt{p-cscf primary ip 10.2.3.4}

The following command enables a P-CSCF with FQDN server name pcscfalias1.ind.pun.cisco.com for the APN:
\texttt{p-cscf fqdn pcscfalias1.ind.pun.cisco.com}

The following command enables a P-CSCF with the IPv4 address 10.2.3.4 at the highest priority of 1 for the APN:
\texttt{p-cscf priority 1 ip 10.2.3.4}
**pco-options**

This command controls the sending of customized PCO (Protocol Configuration Options) options in the network to MS GTP messages and configures APN to include link MTU in PCO IE.

**Product**
- P-GW
- GGSN

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**

```
pco-options { custom1 | ue-requested | link-mtu bytes }  
{ default | no } pco-options [ custom1 | link-mtu ]
```

- **custom1**
  Enable sending of customized PCO options in the network to MS messages; send customized PCO options to all UEs regardless of support.

- **ue-requested**
  Enable sending of customized PCO options in the network to MS messages for "UE-Requested" mode; send PCO to only UEs that request customized PCO options.

- **link-mtu bytes**
  Configures APN to include link MTU in PCO IE, if it is requested by UE.

  When UE sends IPv4 Link MTU Size PCO request during Initial attach/ Standalone PDN connection, then the S-GW/SGSN/HSGW sends the same transparently in Create Session Request, Create/Update PDP Context Request, or PBU to P-GW, GGSN, or PMIP-PGW. Create Session Response, Create/ Update PDP Context Response/ PBA will be sent with latest configured MTU size PCO value in APN. If UE is in outbound roaming, then default value (1500) will be provided in the MTU size PCO.

  *bytes* must be an integer from 1280 to 2000.

  Default: 1500
**Usage Guidelines**

Use this command to enable or disable sending of customized PCO options in the network to MS GTP messages and configure link MTU size PCO value.

- **Important**
  Configure custom PCO values in `pco-custom1` command in *ACS Charging Action Configuration Mode*.

**Examples**

The following command enables sending customized PCO options to all UEs regardless of support:

```
pco-options custom1
```

The following command disables sending of customized PCO options in the network to MS messages and sets the link MTU PCO to 1500 bytes:

```
default pco-options
```
pdn-behavior

Configures specific PDN behavior.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax Description

pdn-behavior { custom1 | ims | lapi }

| default | no | pdn-behavior |

default | no

Configures APN as "Normal".

custom1

Configures APN as a Custom1 (well-known) APN. Re-auth Requested reason code returned for PDN disconnect.

ims

Configures APN as an IMS APN. Re-auth Requested reason code returned for PDN disconnect.

lapi

Configures the APN as a Low Access Priority Indicator (LAPI) APN. Use this command in conjunction with the backoff-timer value command in APN Configuration Mode. Together, they configure the node's behavior for the APN Backoff Timer feature.
Caution

Do not configure the emergency APN and `pdn-behavior lapi` settings in the same APN, as these two settings are mutually exclusive. If both settings are configured in the same APN, the `pdn-behavior lapi` configuration takes priority. As a result, if both settings are configured and the system is overloaded, the call will be rejected. To determine if both settings are configured in the same APN, execute the `show configuration error verbose` command in Exec Mode. The command output contains a warning if both settings are configured in the same APN.

Important

The APN Backoff Timer feature requires that the M2M license be enabled on the P-GW/SAEGW. Contact your Cisco account or support representative for licensing details.

Usage Guidelines

Use this command to configure specific PDN behavior.

Examples

The following command configures APN as an IMS APN which returns reason code Re-auth Requested for PDN disconnect:

```
pdn-behavior ims
```
pdp-type

Configures the type of PDP contexts that are supported by this APN.

**Product**

- GGSN
- P-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-apn)#
```

**Syntax Description**

```
pdp-type {ipv4 [ipv6] | ipv6 [ipv4] | ppp}
```

```
default pdp-type
```

**default**

Configures the default PDP type, IPv4, for the APN.

```
ipv4 [ipv6]
```

Enables support for IPv4 PDP contexts. Also enables support for IPv6 if the IPv6 optional keyword is entered in this command. Default: Enabled

**Important**

Entering both IPv4 and IPv6 in either order enables support for both.

```
ipv6 [ipv4]
```

Enables support for IPv6 PDP contexts. Also enables support for IPv4 if the IPv6 optional keyword is entered in this command. Default: Disabled

**Important**

Entering both IPv4 and IPv6 in either order enables support for both.
**pdp-type**

*ppp*

Enables support for PPP PDP contexts. Default: Disabled

**Usage Guidelines**

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).

**Caution**

For the IPv6 calls to work, the destination context must have at least one IPv6 interface configured.

**Examples**

The following command configures the APN to support PPP context types:

```
pdp-type ppp
```
permission

Enables or disables the ability to use authorized services for the current APN.

**Product**
- P-GW
- SAEGW
- GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```
Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-apn)#
```

**Syntax Description**

| no | permission { nemo | pmipv6-interception } |
|---|---|
| default permission |

- `no` | default
Disables the usage of the specified service.

- `nemo`
Enables the ability to use NEMO functionality.

**Important**
Use of the `nemo` keyword requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

- `pmipv6-interception`
Allows APN to access the external Local Mobility Anchor (LMA) over Proxy Mobile IPv6 (PMIPv6).

**Usage Guidelines**
Use this command to enable support for NEMO or PMIPv6 functionality on the APN. These options are disabled by default.
Examples

The following command enables NEMO functionality:

```
permission nemo
```

The following command disables NEMO functionality:

```
no permission nemo
```
pgw fqdn

Configures both the primary and the secondary FQDN string in the configuration.

**Product**
HSGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-apn) #
```

**Syntax Description**

```
pgw fqdn primary primary-fqdn-name secondary secondary-fqdn-name
default pgw fqdn
no pgw fqdn
```

default
Resets the command to its default setting of disabled.

no
Disables the previously configured pgw fqdn configuration.

**primary primary_fqdn_name**

Configures the primary static fqdn string for the HSGW to select the P-GW.

**secondary secondary_fqdn_name**

Configures the secondary static fqdn string. The primary fqdn will be tried before trying the secondary fqdn.

**Usage Guidelines**

Use this command to configure both the primary and the secondary FQDN string in the configuration.

With with command, DNS resolution is triggered simultaneously for both the primary and secondary P-GW FQDN. Therefore, it is possible for both DNS resolutions to be successful. The focus is on the primary FQDN. However in the case of primary FQDN resolution failure, P-GW selection happens based on the secondary FQDN.
If the above CLI command is not configured then, the HSGW uses DNS to select the serving P-GW. The HSGW receives a list of all the P-GWs that serve the given APN. Then, the HSGW compares a list of P-GWs with the locally configured FQDN and selects the best matching P-GW.

**Examples**

The following command enables the primary FQDN string in the configuration.

`pgw fqdn primary primary-fqdn-name`
policy

Configures the Mobile IPv6 policy to set the action to be taken when IPv4/IPv6 subscriber packets need to be tunneled and the encapsulated packets exceed the tunnel maximum transmission unit (MTU).

Product

P-GW
SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax Description

policy ipv6 tunnel mtu exceed { fragment | inner | notify-sender }
[ default | no ] policy ipv6 tunnel mtu exceed

default
IPv6: System will do a Path MTU (PMTU) discovery and send "ICMPv6 Packet Too Big" to the original sender if the subscriber packet exceeds MTU after encapsulation.
IPv4: System will do an outer IPv6 fragmentation if the packet exceeds MTU after encapsulation.

no
Disables this functionality.

ipv6 tunnel mtu exceed { fragment | inner | notify-sender }
fragment: System will do an outer IPv6 fragmentation if the subscriber packet exceeds MTU after encapsulation.
inner:
IPv6: System will do a PMTU discovery and send "ICMPv6 Packet Too Big" to the original sender if the subscriber packet exceeds MTU after encapsulation.
IPv4: If packet will exceed tunnel MTU after encapsulation, based on DF bit and ignore-Df config, the original IPv4 packet will be fragmented and then encapsulated so that it will not exceed MTU, or ICMP Error will be sent if IPv4 packet fragmentation is not allowed.
notify-sender:
IPv6: System will do a PMTU discovery and send "ICMPv6 Packet Too Big" to the original sender if subscriber packet exceeds MTU after encapsulation.
IPv4: System will do an outer IPv6 fragmentation if packet exceeds MTU after encapsulation.

Usage Guidelines
This command sets the Mobile IPv6 policy for the action to be taken when IPv4/IPv6 subscriber packets need to be tunneled and the encapsulated packets exceed tunnel MTU size.

Examples
The following command causes the system to do outer IPv6 fragmentation if the subscriber packet exceeds MTU after encapsulation:
`policy ipv6 tunnel mtu exceed fragment`
**ppp**

Configures the Point-to-Point Protocol (PPP) options for the current APN.

**Product**

GGSN  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

```plaintext
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-apn)>
```

**Syntax Description**

```plaintext
ppp { data-compression { protocols protocols | mode modes } | keepalive seconds | min-compression-size min_octets | mtu max_octets | l2tp allow-auth-without-pco }  
default ppp { data-compression protocols | keepalive | min-compression-size | mtu | l2tp allow-auth-without-pco }  
no ppp { data-compression protocols | keepalive seconds | mtu | l2tp allow-auth-without-pco }

default

Configures the default PPP parameters for the specified APN.

no

 Resets the option specified to its default setting.

data-compression { mode modes | protocols protocols}

Configures the data compression or the compression protocol to use for the APN. Default: all protocols enabled

**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
Specifies the frequency of sending the Link Control Protocol (LCP) keep alive messages. seconds must be either 0 or an integer from 5 through 14400. The special value 0 disables the keep alive messages entirely. Default: 30

min-compression-size min_octets
Specifies the smallest packet to which compression may be applied as an integer from 0 through 2000. Default: 128

mtu max_octets
Specifies the maximum transmission unit (MTU) for packets accessing the APN as an integer from 100 through 2000. Default: 1500

Important - The MTU refers to the PPP payload which excludes the two PPP octets. Therefore, an MTU of 1500 corresponds to the 3GPP standard MTU of 1502 for GTP packets with PPP payloads.

l2tp
Configures PPP L2TP specific parameters

allow-auth-without-pco
Allows P-GW PPP authentication for a L2TP call to be successful when PCO IE is not received in Create Session Request.

Usage Guidelines
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.

Examples
The following command configures the ppp data-compression mode for the APN to be stateless:
```
ppp data-compression mode stateless
```
The following command configures an MTU of 500 for the APN:
```
ppp mtu 500
```

Examples
The following command configures PPP L2TP specific parameters and allows P-GW PPP authentication for a L2TP call to be successful when PCO IE is not received in Create Session Request:
```
ppp l2tp allow-auth-without-pco
```
proxy-mip

Configures support for Proxy Mobile IP functionality for the APN.

Product
GGSN
FA
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > APN Configuration
\[ \text{configure} > \text{context} \ context\_name > \text{apn} \ apn\_name \]
Entering the above command sequence results in the following prompt:
\[(context\_name)host\_name (config-apn) #\]

Syntax Description
\{ default | no \} proxy-mip \{ required | null-username static-homeaddr \}

default
Configures the default proxy MIP setting for the specified APN

no
Disables this functionality.

required
Default: Disabled.
Enables proxy-mip for all subscribers using this APN.

null-username static-homeaddr
Configures handling of RRQ to enable the acceptance without an NAI extension in this APN. Default: Disabled

Usage Guidelines
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 *GGSN Administration Guide*.

**Examples**

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
```
qci

Specifies the QoS Class Index (QCI) value to be used to mark bearers classified as IMS media for preferential treatment during session recovery and ICSR switchover.

**Product**
- GGSN
- P-GW
- S-GW
- SAE-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

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

**Syntax Description**
```
qci value_bytes ims-media
no qci value_bytes ims-media
```

- **no**
  Disables this IMS QCI feature.

- **ims-media**
  Marks bearers classified as IMS media for preferential treatment during session recovery and ICSR switchover.

- **value_bytes**
  Specifies the QCI value an integer from 1 through 254.

**Usage Guidelines**
Use this command to specify the QCI value to be used to mark bearers classified as IMS media for preferential treatment during session recovery and ICSR switchover.

The following prerequisites apply to the implementation of this feature:

- A dedicated APN must be reserved for VoLTE traffic.
• A call connected to this APN will not be classified as Active VoLTE unless there is a dedicated bearer matching the VoLTE-configured QCI.

• Preferential treatment would be given to only those calls which are active VoLTE.

• A GGSN call connected to this APN will not be classified as Active VoLTE unless there is network initiated bearer matching the VoLTE-configured QCI.

• VoLTE marking is preserved across a Gn-Gp handoff.

When this feature is enabled via a CLI command, the actions are taken:

• During bearer creation
  - New bearer QCI is matched against APN configuration.
  - If the QCI matches an APN configuration, the bearer is marked for preferential treatment.
  - Flow_entries are modified with this information (if this is first VoLTE bearer).
  - Egtpu_session is updated with the VoLTE tag during a rx_setup request.
  - An indication message informs ECS about the VoLTE tagging.

• During bearer deletion
  - Flow_entry is updated with VoLTE information if this is the last VoLTE bearer.
  - ECS is informed of the deletion via an indication message.

Examples
The following command enables preferential treatment for IMS bearers with a QCI of 9:

```
qci 9 ims-media
```
qos negotiate-limit

Cconfigures the QoS profile to provide the peak and committed data rate limits that the GGSN assigns to the APN. The GGSN sends the QoS profile to the SGSNs in response to GTP Create/Update PDP Context requests for traffic shaping and policing functionality.

Product

| GGSN |
| P-GW |
| SAEGW |

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-apn)#`

Syntax Description

`qos negotiate-limit direction { downlink | uplink } [ qci qci_val ] [ peak-data-rate bps ] [ committed-data-rate bps ] [ committed-data-rate { peak-data-rate bps } ]`

`no qos negotiate-limit direction { downlink | uplink } [ qci qci_val ]`

`no`

Disables the QoS Profile for the APN.

`direction { downlink | uplink }`

`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).

`qci qci_val`

`qci_val` is the QoS Class Identifier (QCI) for which the negotiate limit is being set. QCI ranges from 1 to 9. If no qci-val is configured, it will be handled as an undefined-qci (same as undefined-qos class).

`committed-data-rate bps`

Default: See the 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 86400000 for the uplink direction. The value must also correspond to one of the permitted values identified in the tables below. If a non-permitted value is entered for this parameter, 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, 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 (such as, the traffic class is background or interactive), an error occurs if this option is configured. If the committed-rate is applicable (such as, 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 the 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 86400000 for the uplink direction. The value must also correspond to one of the permitted values identified in the tables below. If a non-permitted value is entered for this parameter, 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 Guidelines

This command configures the APN 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 for 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 the tables below.

| Table 19: Permitted Values for Committed and Peak Data Rates in GTP Messages |
|---------------------------------|-------------------|
| **Value (bps)**                 | **Increment Granularity (bps)** |
| From 1000 to 63,000             | 1,000 (e.g 1000, 2000, 3000, ... 63000) |
| From 64,000 to 568,000          | 8,000 (e.g. 64000, 72000, 80000, ... 568000) |
| From 57,6000 to 8,640,000       | 64,000 (e.g. 576000, 640000, 704000, ... 86400000) |
| From 8,700,000 to 16,000,000    | 100,000 bps (e.g. 8700000, 8800000, 8900000, ... 16000000) |
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.

Additional information on the QoS traffic shaping functionality is located in the System Administration Guide.

Default Values:

**Examples**

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

Configures the action on a subscriber traffic flow that violates or exceeds the peak/committed data rate under traffic policing functionality.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-apn) #
```

**Syntax Description**
```
no qos rate-limit direction { downlink | uplink } [ qci qci_val ]
```

no

Disables the QoS data rate limit configuration for the APN.

---

**Important**
When no Qos Profile is configured, the system defaults to using the information provided by the SGSN.

```
qos rate-limit direction { downlink | uplink }

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).

qci qci_val

qci_val is the QoS Class Identifier (QCI) for which the negotiate limit is being set. QCI ranges from 1 to 9. If no qci-val is configured, it will be handled as undefined-qci (same as undefined-qos class).
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.

\textit{bytes} must be an integer from 1 through 6000000.

\begin{itemize}
  \item \textbf{Important} \hspace{1em} It is recommended that the minimum value of this parameter be configured to the greater of the following two values: 1) three 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.
\end{itemize}

\textbf{auto-readjust [ duration dur ]} keyword provides the option to calculate the Burst size dynamically while configuring the rate-limit. Whenever this keyword is enabled to calculate burst size, the GGSN QoS negotiated rate is enforced for this calculation.

Whenever there is a change in the rates (due to a QoS update), 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.

\textit{duration dur} describes the duration of burst in seconds. If duration is not specified this keyword will use 1 second as default value.

\textit{dur} must be an integer between 1 through 30.

\textbf{exceed-action \{ drop \| lower-ip-precedence \| transmit \} }

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:

\begin{itemize}
  \item \textbf{drop}: Drop the packet.
  \item \textbf{lower-ip-precedence}: Transmit the packet after lowering the ip-precedence.
  \item \textbf{transmit}: Transmit the packet.
\end{itemize}

\textbf{violate-action \{ drop \| lower-ip-precedence \| shape \| transmit-when-buffer-full \| transmit \} }

The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

\begin{itemize}
  \item \textbf{drop}: Drop the packet.
  \item \textbf{lower-ip-precedence}: Transmit the packet after lowering the IP precedence.
  \item \textbf{shape [ transmit-when-buffer-full ]}: This keyword is not supported in this release.
  \item \textbf{transmit}: Transmit the packet.
\end{itemize}

\begin{itemize}
  \item \textbf{Important} \hspace{1em} Traffic Shaping is not supported on the GGSN, P-GW, or SAEGW.
\end{itemize}
More than one of the above keywords can be entered within a single command.

**Usage Guidelines**

This command configures APN quality of service (QoS) through traffic policing. This command enables the actions on subscriber flows exceeding or violating the allowed peak/committed data rate.

**Important**

This command is not intended for bearer level policing

**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 this 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. (It accepts all of the SGSN-provided values for the PDP context.)

To calculate the burst size dynamically, an optional keyword **auto-readjust [ duration dur ]** is provided with the **burst-size** keyword. By default, the burst size is fixed if defined in bytes with this command. Regardless of the rate being enforced, burst-size is fixed as set by the **burst-size bytes** parameter.

The **auto-readjust [ duration dur ]** keyword enables variable burst size depending on the rate being enforced. The system calculates burst size using a 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 the **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 regardless of the rate being enforced.

If the **auto-readjust** keyword is provided without specifying the duration, a default duration of 1 second will be used for burst size calculation.

**Examples**

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-renegotiate

This command is obsolete.
qos traffic-police

This command is obsolete. This functionality is now supported through `qos negotiate-limit` and `qos rate-limit` commands.

**Command Modes**

- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-apn)#
```
radius

This command is obsolete.
radius group

This command is obsolete.
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
- P-GW
- SAEGW

Privilege
Security Administrator, Administrator

Command Modes
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax Description
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 supplies framed IP address as 255.255.255.255 and the MS does not supply an address.

{ accept-call-when-ms-ip-not-supplied | reject-call-when-ms-ip-not-supplied }

accept-call-when-ms-ip-not-supplied: Accept calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address.

reject-call-when-ms-ip-not-supplied: Reject calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address.

Usage Guidelines
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.
Examples

Use the following command to set the APN to reject calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address:

```
radius returned-framed-ip-address 255.255.255.255-policy reject-call-when-ms-ip-not-supplied
```
radius returned-username

Configures the username that is returned in accounting messages. If the username is not available in the Protocol Configuration Options (PCO), the RADIUS returned username is preferred to the constructed username (imsi@apn, msisdn@apn, or outbound username).

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax Description
radius returned-username { override-constructed-username | prefer-constructed-username }

default radius returned-username

default

The default value for the RADIUS returned-username is prefer-constructed-username. The constructed username (imsi@apn, msisdn@apn) will be used.

Important
If the username is available in the PCO, that username will be used regardless of the setting for this command (radius returned-username).

override-constructed-username

If the RADIUS server returns a username in the Access-Accept message and that username is not available in the Protocol Configuration Options (PCO), the new username from the RADIUS server will be used.

prefer-constructed-username

If the username is not available in the PCO, a constructed username (imsi@apn, msisdn@apn) will be used regardless of the username from the RADIUS server. This is the default.
**Usage Guidelines**

Use this command to configure the username that is returned in accounting messages.

**Examples**

Following command sets the default value for the RADIUS returned-username is prefer-constructed-username

constructed username (imsi@apn, msisd@apn):

```
default radius returned-username
```
radius rulebase-format

This command enables/disables the Rulebase Concatenation feature at APN level. This feature is used to merge the prepaid attribute and SN1-Rulebase as a new rulebase and then apply the new rulebase to the session. If the Rulebase Concatenation feature is not enabled, the last received rulebase is applied to the session.

Important This command is license dependent. For more information, contact your Cisco account representative.

Product
- GGSN
- PDSN
- P-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn) #

Syntax Description
- radius rulebase-format { custom1 | standard }
- default radius rulebase-format standard

default
Disables the Rulebase Concatenation feature. The default setting is standard.

custom1
Specifies the rulebase as a custom value derived from multiple RADIUS attributes in the RADIUS Access-Accept response message.

standard
Specifies the rulebase as a single attribute value as obtained in RADIUS Access-Accept response message. This is the default setting.
Usage Guidelines

Currently, the Wireless Mobile Private Network (MPN) configures a dedicated rulebase per service. The Enterprise that utilizes this service has the rulebase per subscriber in 3G or signaled from AAA server with SN1-Rulebase attribute. In the case of a prepaid service, the rulebase name will be the customer-specific prepaid policy attribute received from the AAA server.

When both the RADIUS attributes are received, the last received attribute is considered and applied to the subscriber session. This CLI command is used to merge prepaid attribute and SN1-Rulebase as a new rulebase and then apply the new rulebase to the session on the gateway.

Important

Rulebase Concatenation is a customer-specific feature and it requires a valid license to enable the feature. For more information, contact your Cisco account representative.

In 18 and earlier releases, rulebase was a single attribute value as obtained in the RADIUS Access-Accept response message. That is, only one rulebase can be applied with either SN1-Rulebase AVP or customer-specific prepaid policy AVP, whichever comes last.

In 19 and later releases, when both the attributes are received, the rulebase name will be a concatenation of the attributes as received in the Access-Accept response message. If only one of the attributes is received, the current behavior is applicable i.e. the last received attribute will be selected as the rulebase and it will be applied to the session.

If the concatenated rulebase is not matching with the rulebase configured on the gateway, and/or if both the attributes are present more than once, then the session is rejected.

This feature implementation helps the MPN to customize the rulebase and combine prepaid service with additional services like Service Based Access (SBA).

Examples

The following command merges the RADIUS attributes and installs the new concatenated rulebase.

```
radius rulebase-format custom1
```
**reporting-action**

Enables the reporting of APN-related events to a log. By default, reporting events to a log is disabled.

**Product**
P-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**

```
[ default | no ] reporting-action event-record
```

default
Disables reporting of events to a log. By default, reporting is disabled.

no
Disables reporting of events to a log if reporting has been enabled.

**Usage Guidelines**

Use this command to enable the reporting of APN-related events to a log. By default, reporting is disabled.

**Examples**
The following command enables reporting of events to a log:

```
reporting-action event-record
```
restriction-value

Configures the level of restriction to ensure controlled co-existence of the Primary PDP Contexts.

Product
- GGSN
- P-GW
- SAEGW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name
Entering the above command sequence results in the following prompt:
(context_name)host_name(config-apn)#

Syntax Description
restriction-value value
[ default | no ] restriction-value

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.

value
Specifies a unique number that identifies the type of network supported for primary PDP contexts facilitated by this APN. The following values are supported:

- 1: Value used for Wireless Application Protocol (WAP) or Multimedia Messaging Service (MMS) type of networks. This corresponds to APN type public-1.
- 2: Value used for Internet or Packet-Switched Public Data Network (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.
**Usage Guidelines**

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 the total number of Primary PDP Contexts 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, then 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.

**Examples**

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 Network Address Translation (NAT).

---

**Important**

This command is license dependent. For more information please contact your Cisco account representative.

---

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

`{context_name}@host_name(config-apn)#`

---

**Syntax Description**

`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 alphanumeric string of 1 through 31 characters.

**Usage Guidelines**

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.

**Examples**

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 mobile station's subscription to use this APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-apn)#
```

**Syntax Description**
```
selection-mode { chosen-by-sgsn | sent-by-ms | subscribed } +
default selection-mode
```

**default**
Sets the default selection mode as "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 Guidelines**

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).

**Examples**

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
```
stats-profile

Associates a statistics profile with a configured APN to support the Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters feature.

**Important**
ARP Granularity for QCI Level Counters is a license-controlled feature. Per QCI Packet Drop Counters functionality does not require a license. Contact your Cisco account or support representative for licensing details.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration
```
configure > context context_name > apn apn_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-apn)#
```

**Syntax Description**
- `| no | stats-profile stats_profile_name`

- `no`
  disassociates the statistics profile with the specified APN.

- `stats-profile stats_profile_name`
  Specifies the existing statistics profile to associate with this APN. Statistics profiles are configured in Global Configuration Mode with the `stats-profile` command.

**Usage Guidelines**
Statistics profiles enable operators to monitor QoS statistics that identify multiple services running with the same QCI value. In addition, packet drop counters have been introduced to provide the specific reason the Enhanced Charging Service (ECS) dropped a packet. The packet drop counters provide output on a per ARP basis. This provides additional information that operators can use to troubleshoot and identify network issues that may be affecting service.
For detailed information on this feature, refer to the "Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters" chapter in the P-GW Administration Guide or the SAEGW Administration Guide.

**Examples**

The following command associates the stats-profile STATS with the APN:

```
stats-profile STATS
```
timeout

Configures the session timeout values for this APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
 Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-apn)#
```

**Syntax Description**
```
timeout { absolute | qos-renegotiate } time [ del-cause { none | reactiv-req } ]
[ default | no ] timeout [ absolute | qos-renegotiate ] [ del-cause ]
```

- **default**
  Set the default value for the followed option.

- **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.

- **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-renegotiation = 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.

**del-cause { none | reactiv-req }**

When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include "Cause-IE" in the resulting Delete Bearer/Delete PDP Context Requests generated for default bearer.

**none**: Omit GTP "Cause-IE" in DBR/DPC when timeout occurs on default bearer.

**reactiv-req**: The DBR/DPC will include "Cause-IE" with GTP cause code "Reactivation Requested".

This behavior is applicable only if Delete Bearer Request is sent for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.

The behavior for "Cause-IE" specified in this CLI shall override the cause-code set by existing features. By default, the **del-cause** option is not defined and existing behavior is retained.

---

**Important**

This option is only valid when Cause IE Enhancement for Delete Bearer Request license is enabled. Contact your Cisco account representative for more information.

---

**Usage Guidelines**

Use this command to limit the amount of time that a subscriber session can remain connected or as a QoS renegotiation dampening timer.

**Examples**

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 through an APN. The bearer inactivity timer can also be configured to exclude default bearer/primary bearer from monitoring bearer inactivity.

**Product**

GGSN
P-GW
SAEGW
SGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**

In StarOS 15.0 and later releases:

```
timeout bearer-inactivity [ gbr | non-gbr ] dur_seconds volume-threshold { downlink | total | uplink } bytes
```

```
timeout bearer-inactivity del-cause { none | reactiv-req }
```

```
timeout bearer-inactivity exclude-default-bearer
[ default | no ] timeout bearer-inactivity [ del-cause | exclude-default-bearer | gbr | non-gbr ]
```

In StarOS 14.x and earlier releases:

```
timeout bearer-inactivity dur_seconds volume-threshold total bytes
```

```
default
```

Sets the bearer inactivity timer to disabled mode.

```
no
```

Removes the configured bearer inactivity timer values and traffic threshold limit.

```
timeout
```

Specifies that a bearer time out value will be configured for this APN.
**gbr**
Specifications that the GGSN/GW will check for low activity on a GBR bearer.

**non-gbr**
Specifications that the GGSN/GW will check for low activity on a non-GBR bearer.

---

**Important**
P-GW only supports non-GBR bearer type sessions.

---

**dur_seconds**
Specifies the timeout duration in seconds to check inactivity on the bearer.

In StarOS 16.0 and later releases:

`dur_seconds` must be an integer value from 300 to 2592000 (5 minutes to 720 hours). The minimum configurable value of bearer inactivity timer was reduced from 900 seconds to 300 seconds.

In StarOS 15.0 releases:

`dur_seconds` must be an integer value from 900 to 2592000 (15 minutes to 720 hours). The minimum configurable value of bearer inactivity timer was reduced from 3600 seconds to 900 seconds.

In StarOS 14.x and earlier releases:

`dur_seconds` must be an integer value from 3600 through 2592000.

**volume-threshold**
This keyword sets the volume threshold in bytes to check the low activity on the bearer.

**downlink**
Threshold value of the downlink data traffic in a bearer.

**total**
Specifies that the total of both uplink and downlink data will be used as a volume threshold.

**uplink**
Threshold value of the uplink data traffic in a bearer.

**bytes**
`bytes` must be an integer value from 1 through 4294967295.

**del-cause { none | reactiv-req }**
When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include "Cause-IE" in the resulting Delete Bearer/Delete PDP Context Requests generated for default bearer.

**none**: Omit GTP "Cause-IE" in DBR/DPC when timeout occurs on default bearer.

**reactiv-req**: The DBR/DPC will include "Cause-IE" with GTP cause code "Reactivation Requested".
This behavior is applicable only if Delete Bearer Request is sent for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.

The behavior for "Cause-IE" specified in this CLI shall override the cause-code set by existing features. By default, the **del-cause** option is not defined and existing behavior is retained.

---

**Important**

This option is only valid when Cause IE Enhancement for Delete Bearer Request license is enabled. Contact your Cisco account representative for more information.

---

**exclude-default-bearer**

Ignore bearer inactivity handling for default/primary bearer.

---

**Usage Guidelines**

Use this command to configure the bearer inactivity timer and the threshold value of the traffic through an APN. This enables the deletion of bearers experiencing less data traffic than the configured threshold value. Bearer inactivity timer is started only when time and volume threshold is configured.

---

**Important**

Only one threshold is allowed to be configured per APN which is to monitor total, uplink, or downlink traffic.

The bearer inactivity timer can also be configured to exclude default bearer/primary bearer from monitoring bearer inactivity.

---

**Examples**

The following command enables the inactivity time on the bearer with a timeout duration of 7200 seconds and the total traffic volume of 256000 bytes in uplink and downlink directions as thresholds:

```
timeout bearer-inactivity 7200 volume-threshold total 256000
```
timeout emergency-inactivity

Configures the emergency session inactivity-timeout for this APN. The APN must be configured as an emergency APN for Voice over LTE (VoLTE) E911 support.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:
{context_name}@host_name(config-apn)#

**Syntax Description**

timeout emergency-inactivity seconds

| default | no | timeout emergency-inactivity |

default | 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.

seconds
Default: 0 (disabled)

Specifies the timeout duration, in seconds, to check inactivity on the emergency session.
seconds must be an integer value from 1 through 3600.

**Usage Guidelines**

Use this command to set the emergency session inactivity-timeout for this APN.

At reception of an IP CAN Session Modification Request triggered by the Policy and Charging Rules Function (PCRF) for an IP-CAN (IP Connectivity Access Network) session serving an IMS emergency session that removes all PCC rules with a QCI other than the default bearer QCI and the QCI used for IMS signalling, the Policy and Charging Enforcement Function (PCEF) shall start a configurable inactivity timer (to enable PSAP Callback session). When the configured period of time expires, the PCEF shall initiate an IP-CAN Session Termination Request for the IP-CAN session serving the IMS Emergency session.

If a PCRF-Initiated IP-CAN Session Modification Request provides new PCC rule(s) with a QCI other than the default bearer QCI and the QCI used for IMS signalling, the PCEF shall cancel the inactivity timer.
Refer to the `emergency-apn` command in this chapter for additional information.

Examples

The following command sets the emergency inactivity timeout duration to 450 seconds.

`timeout emergency-inactivity 450`
timeout idle

Configures the idle timeout duration for the long duration timer associated with a subscriber session.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

```plaintext
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-apn)#
```

**Syntax Description**

```plaintext
timeout idle idle_dur [ del-cause { none | reactiv-req } ]
[ default | no ] timeout idle [ del-cause ]
```

**default | 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 expiry the system considers the session as dormant or idle and terminates the session.

**idle_dur** must be an integer value in the range from 0 through 4294967295.

The special value 0 disables the timeout specified.

**del-cause { none | reactiv-req }**

When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include "Cause-IE" in the resulting Delete Bearer/Delete PDP Context Requests generated for default bearer.

**none**: Omit GTP "Cause-IE" in DBR/DPC when timeout occurs on default bearer.

**reactiv-req**: The DBR/DPC will include "Cause-IE" with GTP cause code "Reactivation Requested".

This behavior is applicable only if Delete Bearer Request is sent for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.

The behavior for "Cause-IE" specified in this CLI shall override the cause-code set by existing features.
By default, the **del-cause** option is not defined and existing behavior is retained.

**Important**  
This option is only valid when Cause IE Enhancement for Delete Bearer Request license is enabled. Contact your Cisco account representative for more information.

**Usage Guidelines**  
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.

**Examples**  
Following command sets the idle timeout duration to 450 seconds.  
`timeout idle 450`
**timeout idle micro-checkpoint-deemed-idle**

Sends an event-based idlesec micro-checkpoint from an Active to a Standby chassis when the session state changes from active to idle or from idle to active.

**Product**

All

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-apn)#
```

**Syntax**

```
timeout idle idle_dur | micro-checkpoint-deemed-idle time_in_seconds |
{ default | no } timeout idle
```

**default**

Indicates the timeout specified is to be returned to its default behavior.

**no**

Disables the timeout idle functionality.

**timeout idle idle_dur**

Designates the maximum duration of the session (in seconds). After expiry, the system considers the session as dormant or idle and terminates the session.

`idle_dur` must be an integer value in the range from 0 through 4294967295.

Default: 0

The special value 0 disables the timeout specified.

**micro-checkpoint-deemed-idle time_in_seconds**

Specifies the time duration, in seconds, after which a session state is deemed to have changed from active to idle or idle to active, and a micro-checkpoint is then sent from the active to the standby chassis.

`time_in_seconds` must be an integer from 10 to 1000.

Default: 180
The **micro-checkpoint-deemed-idle** value should be less than the **timeout idle** value.

**Usage Guidelines**

Use **micro-checkpoint-deemed-idle** to send an idlesec micro-checkpoint from an active to standby chassis when the session state changes from active to idle or from idle to active. The micro-checkpoint carries information about the time when the session became active or idle. Upon receipt of the micro-checkpoint, the standby chassis updates the active/idle time. This process enables the active and standby chassis to be synchronized with respect to when a particular session became active or idle. Since this feature is event-based, it enables the chassis to send micro-checkpoints only when an event occurs, as opposed to sending micro-checkpoints based on a configured time duration, which sends the micro-checkpoints regardless of whether a session state change occurred or not.

Using **micro-checkpoint-deemed-idle** results in a more efficient event-based sending of micro-checkpoints to the standby chassis and also increases SRP bandwidth.

**Important** Either the **micro-checkpoint-deemed-idle** or **micro-checkpoint-periodicity** value can be configured for idle time duration. Any change from **micro-checkpoint-deemed-idle** to **micro-checkpoint-periodicity**, or vice versa, requires removing the first configuration before adding the new configuration.

**Examples**

This command sets the **timeout idle** value to 300 seconds and the **micro-checkpoint-deemed-idle** setting to 180 seconds.

```
timeout idle 300 micro-checkpoint-deemed-idle 180
```
timeout idle micro-checkpoint-periodicity

Enables configuration of periodic idle seconds micro checkpoint timer on a per-APN basis.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-apn)#
```

**Syntax Description**

```
timeout idle idle_dur | micro-checkpoint-periodicity time_in_seconds | 
{ default | no } timeout idle
```

**default**

Indicates the timeout specified is to be returned to its default behavior.

**no**

Disables the timeout idle functionality.

**idle_dur**

Designates the maximum duration of the session (in seconds). After expiry, the system considers the session as dormant or idle and terminates the session.

**idle_dur** must be an integer value in the range from 0 through 4294967295.

Default: 0

The special value 0 disables the timeout specified.

**micro-checkpoint-periodicity time_in_seconds**

Configures periodic idle seconds micro-checkpoint timer on a per-APN basis.

Idle seconds micro-checkpoints are sent at the configured regular intervals to the standby chassis; otherwise, they are sent at intervals of 10 seconds, which is the default value.

**time_in_seconds** must be an integer value in the range from 0 through 4294967295.

Default: 10
Important The **micro-checkpoint-periodicity** value should be less than **idle timeout** value.

**Usage Guidelines**

Use this command to set the idle time duration and micro-checkpoint-periodicity timer for subscriber session to determine the dormant session. Operators can configure this setting to a large value to suit their need to reduce the number of micro-checkpoints on the SRP link. When this CLI command is configured, idle seconds micro-checkpoints are sent at configured regular intervals to the standby chassis. If not configured, micro-checkpoints are sent at intervals of 10 seconds, which is the default.

Important Either the **micro-checkpoint-deemed-idle** or **micro-checkpoint-periodicity** value can be configured for idle time duration. Any change from **micro-checkpoint-deemed-idle** to **micro-checkpoint-periodicity**, or vice versa, requires removing the first configuration before adding the new configuration.

**Examples**

Following command sets the idle timeout duration to 10 seconds and micro-checkpoint-periodicity to 15 seconds.

timeout idle 10 micro-checkpoint-periodicity 15
timeout long-duration

Configures the long duration timeout and inactivity duration for subscriber sessions.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:
{context_name}host_name(config-apn)#

Syntax Description

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 timeouts are set to their default behavior.

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 initiated.
ldt_timeout must be an integer 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 an integer value in the range from 0 through 4294967295.
The special value 0 disables the inactivity time specified.
**Usage Guidelines**

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` commands in this chapter for additional information.

**Examples**

The following command sets the long duration timeout duration to 300 seconds and the inactivity timer for subscriber session to 45 seconds.

```
timeout long-duration 300 inactivity-time 45
```
The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
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
SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn) #

Syntax Description

tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }
default tunnel address-policy

default

Resets the tunnel address-policy to alloc-validate.

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 arriving via L3 tunnels. Incoming static IP addresses are passed. This allows for the greatest flexibility.
**Usage Guidelines**

This command supports scalable solutions for Corporate APN deployment as many corporations handle their own IP address assignments. 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 `l3-to-l2-tunnel address policy` as defined in the APN Configuration mode, will be in effect.

**Examples**

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
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-apn)#`

**Syntax Description**

`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 IPv4 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 Guidelines

Subscriber IP payloads are encapsulated with IP/GRE headers and tunneled by the GGSN to an external gateway.

Examples

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 preference 1
**tunnel ipip**

Configures IP-in-IP tunnelling parameters between the GGSN and an external gateway for the APN.

**Product**

GGSN  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-apn)#
```

**Syntax Description**

`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 IPv4 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 IPv4 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 Guidelines

Subscriber IP payloads are encapsulated with IP-in-IP headers and tunneled by the GGSN to an external gateway.

Examples

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 preference 1
tunnel ipsec

This command configures sessions for the current APN to use an Internet Protocol Security (IPSec) tunnel based on the IP pool corresponding to the subscribers assigned IP address.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax Description**

| no | tunnel ipsec use-policy-matching-ip-pool |

**Usage Guidelines**

Use this command to set the APN to use an IPSec policy that is assigned to the IP pool that the subscribers assigned IP address relates to.

**Examples**

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
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-apn)#
```

**Syntax Description**
```
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
```

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.

**peer-address lns-address**

Specifies the IP address of the LNS node that the LAC service connects to.

*lns-address must be expressed in IPv4 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 L2TP Access Concentrator (LAC) service (configured on the system) and the LNS node.
l2tp_secret must be an alphanumeric string of 1 through 127 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 an alphanumeric string of 1 through 79 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 IPv4 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 the "tunnel l2tp" command in the APN for the LNS peer will be used as a LAC Hostname.
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 alphanumeric string of 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, the 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 expressed as an alphanumeric string of 1 through 127 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 0 to 255 bytes.

**Usage Guidelines**

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.

**Examples**

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 gdcr

This command defines which APN (Gn or virtual) should be used in charging records.

**Product**
- eWAG
- GGSN
- IPSG
- P-GW
- SAEGW

**Privilege**
- Security Administrator
- Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)
```

**Syntax Description**

```
virtual-apn gdcr apn-name-to-be-included { gn | virtual }
default virtual-apn gdcr apn-name-to-be-included

default
```

Returns the CDR related parameters to the default values.

```
gdcr apn-name-to-be-included { gn | virtual }
```

Defines which APN is to be sent in charging records (CDR).

- **gn**: Use the Gn APN name received in the Create PDP Context Request message from SGSN or the S5 APN name received in the PDN Connectivity Request from MME.
- **virtual**: Use the virtual APN selected by the GGSN/P-GW. This is the default.

**Usage Guidelines**

Defines which APN is to be sent in charging records (CDR), either the APN received in the Create PDP Context Request from the SGSN, or the APN received in the PDN Connectivity Request from the MME.
Examples

The following command configures the gateway to use the APN supplied by the SGSN or MME.

virtual-apn gdcr apn-name-to-be-included gn
**virtual-apn preference**

Defines one or more criteria used to redirect a call received on a particular APN to another APN.

**Product**
- GGSN
- eWAG
- IPSG
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)##
```

**Syntax Description**
In StarOS 20.2 and later releases:

```
virtual-apn preference priority apn apn_name [ IPv4 { ip_address | ipv4_address/mask } | IPv6 ipv6_address | ipv6_address/mask } | [ bearer-access-service service_name | cc-behavior cc_behavior_value | cc-profile cc_profile_index | pre-rel-9.1-cc-behavior cc_behavior_value | [ domain domain_name | mcc mcc_number mnc mnc_number | msin-range from msin_range_from to msin_range_to | msisdn-range from msisdn_start_range to msisdn_to_range | pdp-type { ipv4 | ipv6 | ipv4v6 } | rat-type { eutran | gan | geran | hspa | utran | wlan } | roaming-mode { home | roaming | visiting } | serv-gw-plmnid mcc mcc_number mnc mnc_number ] +
```

no virtual-apn preference priority

In StarOS 20.1 and earlier releases:

```
virtual-apn preference priority apn apn_name [ IPv4 { ip_address | ipv4_address/mask } | IPv6 ipv6_address | ipv6_address/mask } | [ bearer-access-service service_name | cc-behavior cc_behavior_value | rat-type { eutran | gan | geran | hspa | utran | wlan } | [ cc-profile cc_profile_index | pre-rel-9.1-cc-behavior cc_behavior_value | rat-type { eutran | gan | geran | hspa | utran | wlan } | domain domain_name | mcc mcc_number mnc mnc_number | cc-behavior cc_behavior_value | cc-profile cc_profile_index | pre-rel-9.1-cc-behavior cc_behavior_value | msin-range from msin_range_from to msin_range_to | rat-type { eutran | gan | geran | hspa | utran | wlan } | msisdn-range from msisdn_start_range to msisdn_to_range | pdp-type { ipv4 | ipv6 | ipv4v6 } | roaming-mode roaming | rat-type { eutran | gan | geran | hspa | utran | wlan } | roaming-mode
```

---

Command Line Interface Reference, Commands A - B, StarOS Release 20
virtual-apn preference

no virtual-apn preference priority

no
Removes a previously configured "virtual" APN.

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 or PDN connections with matching properties.

apn_name is the name of the alternative APN expressed as an alphanumeric string of 1 through 62 alphanumeric characters and is case insensitive. It may also contain dots (.) and/or dashes (-).

IPv4 { ipv4_address | ipv4_address/mask }
Configures subnet range for subscriber IP.

ipv4_address must be an IPv4 address in dotted-decimal notation.

ipv4_address/mask must be an IPv4 address in dotted-decimal notation with network-host mask separation.

IPv6 { ipv6_address | ipv6_address/mask }
Configures subnet range for subscriber IP.

ipv6_address must be an IPv6 address in colon-separated-hexadecimal notation.

ipv6_address/mask must be an IPv6 address in colon-separated-hexadecimal notation with network-host mask separation.

access-gw-address { ip_address | ip_address/mask }
Specifies the Access Gateway (SGSN/S-GW/Other) IP address (or network) for this virtual APN.

ip_address must be an IPv4 address in dotted-decimal or an IPv6 address in colon-separated-hexadecimal notation.

ip_address/mask must be an IPv4 address in dotted-decimal or an IPv6 address in colon-separated-hexadecimal notation with network-host mask separation.

bearer-access-service service_name
Specifies the Bearer Access Service (GGSN/P-GW/Other) name. This service name is unique across the context.

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

Important
For eWAG and IPSG, this option is not supported in this release.
**cc-behavior cc_behavior_value**

Specifies the behavior charging characteristics bits in 16 bit format, post 3GPP release 9.1. For example, if cc-behavior is configured as 0x3412, then 0x34 corresponds to B15-B8 [MSB] and 0x12 corresponds to B7-B0 [LSB] of charging char.

*cc_behavior_value* must be a hex value in the range 0x0000 to 0xFFFF.

---

**Important**

This option is supported only on GGSN, P-GW, and SAEGW in this release.

**cc-profile cc_profile_index**

Specifies the charging characteristics (CC)-profile index.

*cc_profile_index* must be an integer from 1 to 15.

---

**Important**

For eWAG and IPSG, this option is not supported in this release.

**domain domain_name**

Specifies the domain name (realm). This is compared with the domain name portion of subscriber's username (user@domain).

*domain_name* must be an alphanumeric string of 1 through 79 characters, is case sensitive and can contain all special characters.

---

**Important**

For eWAG and IPSG, this option is not supported in this release.

**mcc mcc_number mnc mnc_number**

**mcc**: 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 3-digit integer value between 100 and 999.

**mnc**: 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.

---

**Important**

For eWAG and IPSG, this option is not supported in this release.

**msin-range from msin_range_from to msin_range_to**

---

**Important**

This option is supported only for the GGSN.
Specifies the IMSI MSIN range.

\textit{msin\_range\_from} is the start prefix of the IMSI MSIN range and can be configured between 0 and 9999999999.

\textit{msin\_range\_to} is the end prefix of the IMSI MSIN range and can be configured as a string of size 1 to 10 digits between 0 and 9999999999.

\textit{msin\_range} should obey the following rules:

- Start prefix (such as \textit{msin\_range\_from}) and end prefix (such as \textit{msin\_range\_from}) must be of the same length.
- Total length of \textit{mcc + mnc + msin\_range} <= 15 digits.

\textbf{msisdn\_range from msisdn\_start\_range to msisdn\_to\_range}

Specifies the MSISDN range.

\textit{msisdn\_start\_range} is the starting MSISDN number which a string of size 2 to 15 and its value ranges between 00 and 999999999999999.

\textit{msisdn\_to\_range} is the ending MSISDN number which is also a string of size 2 to 15 and its value ranges between 00 and 999999999999999.

\textbf{Important}

For eWAG, this option is not supported in this release.

\textbf{pre-rel-9.1-cc-behavior \textit{cc\_behavior\_value}}

Specifies the behavior charging characteristics bits in 12 bit format, post 3GPP release 9.1. For example, if \textit{cc-behavior} is configured as 0x341, then 0x34 corresponds to B12-B5 [MSB] and 0x1 corresponds to B4-B1 [Least significant nibble] of CC behavior.

\textit{cc\_behavior\_value} must be a hex value in the range 0x0000 to 0xFFFF.

\textbf{Important}

This option is supported only on GGSN, P-GW, and SAEGW in this release.

\textbf{pdp-type \{ ipv4 | ipv4v6 | ipv6n \}}

Configures pdp-type rule.

The available options include:

- \textit{ipv4}: Configures VAPN Rule for IPv4.
- \textit{ipv4v6}: Configures VAPN Rule for IPv4v6.
- \textit{ipv6}: Configures VAPN Rule for IPv6.

\textbf{rat-type \{ eutran | gan | geran | hspa | utran | wlan \}}

The type of the Radio Access Technology (RAT).

The available options include:

- \textit{eutran}
• gan
• geran
• hspa
• utran
• wlan

**Important** For eWAG, the rat-type keyword is not supported in this release.

roaming-mode { home | roaming | visiting }

Supports separate PDP context or PDN connection processing for roaming, visiting, and home subscribers.

**Important** For eWAG and IPSG, this option is not supported in this release.

**serv-gw-plmnid**

Specifies the Serving Gateway PLMN ID.

+ Keywords can be repeated or combined as needed in a single virtual-apn preference rule.

If the same option is provided multiple times in the same rule, then later option value will be considered for selection.

**Usage Guidelines**

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 or PDN connections are compared against and a priority that dictates the comparison order.

A maximum of 2048 virtual APN rules can be added across all APNs.

**Important** To modify an existing virtual APN rule, the current rule should be removed and a new rule with appropriate options added.

**GGSN**

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 determines 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 criteria (domain name, mcc/mnc, etc.), the "virtual" APN reference should refer to an APN that is not configured on the system and contains the desired rule. All calls matching the configured rule would then be denied with a reason code of 219 (DBH), Missing or Unknown APN.

eWAG

For eWAG, in this release only the access-gw-address Virtual APN configuration option is supported.

For information on how virtual APN configuration can be used in eWAG deployments, refer to the Enhanced Wireless Access Gateway Administration Guide.

IPSG

For IPSG, in this release only the following Virtual APN configuration options are supported:

- access-gw-address (RADIUS client in the case of IPSG)
- msisdn-range from msisdn_start_range to msisdn_to_range
- rat-type

All these attributes are sent in access-request in Auth-Proxy mode or Acct-Start in other modes to trigger Virtual APN selection.

The functionality provided by this command can also be used to restrict access to particular APNs. To restrict access based on a particular criteria (domain name, mcc/mnc, etc.), the "virtual" APN reference should refer to an APN that is not configured on the system and contains the desired rule. All calls matching the configured rule would then be denied with a reason code of 219 (DBH), Missing or Unknown APN.

P-GW/SAEGW

The Virtual APN feature allows a carrier to use a single APN to configure differentiated services. The APN that is supplied by the MME is evaluated by the P-GW in conjunction with multiple configurable parameters. Then, the P-GW selects an APN configuration based on the supplied APN and those configurable parameters.

APN configuration dictates all aspects of a session at the P-GW. Different policies imply different APNs. After basic APN selection, however, internal re-selection can occur based on the following parameters:

- S-GW address: access-gw-address
- Service name: bearer-access-service
- Call control profile index: cc-profile
- Domain name part of username (user@domain): domain
- MCC-MNC of IMSI: mcc mcel_number mnc mnc_number
• MSISDN range: **msisdn-range** from **msisdn_start_range** to **msisdn_to_range**

• Subscriber type: **rat-type**

---

**Important**

In StarOS v12.x and earlier, the P-GW supports a maximum of 1024 Virtual APNs in a system. In StarOS v14.0 and later, the P-GW supports a maximum of 2048 Virtual APNs in a system.

The functionality provided by this command can also be used to restrict access to particular APNs. To restrict access based on a particular criteria (domain name, mcc/mnc, etc.), the "virtual" APN reference should refer to an APN that is not configured on the system and contains the desired rule. All PDN connections matching the configured rule would then be denied with a reason code of 219 (DBH), Missing or Unknown APN.

---

**Examples**

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.

```
virtual-apn preference 1 apn bigco domain bigco.com
virtual-apn preference 2 apn bigtown mcc 100 mnc 50 msin-range from 4000000000 to 4999999999
virtual-apn preference 3 apn bigco.com access-gateway-address 192.168.62.2
virtual-apn preference 4 apn bigco.co.kr access-gateway-address 192.168.60.2/24
```
virtual-apn preference
APN Remap Table Configuration Mode

Important

Beginning with Release 16 for SGSN only, an APN Remap Table associated with an IMEI profile overrides a remap table associated with an operator policy. This means activation will be rejected if a local default APN configured, in an APN Remap Table associated with an IMEI profile, cannot be used. This will occur even if a valid local default APN is available in an APN Remap Table associated with an operator policy.

A maximum of 1,000 APN remap tables are supported, and each APN remap table supports a maximum of 100 APN remap entries. Multiple tables can be defined and stored but an operator policy and/or IMEI profile each only support association with a single (one) table per policy/profile configuration. The APN remap table associated with an IMEI profile will be used in IMEI override scenarios.

APN Remap Table Configuration mode provides the commands to configure parameters for multiple features related to Access Point Name (APN) handling, such as: Default APN, APN Remap, and Wildcard APN. APN remap table is a key element of the Operator Policy feature and a table is not usable (valid) until it has been associated with an operator policy (see the Operator Policy Configuration Mode Commands) or an IMEI profile (see the IMEI Profile Configuration Mode Commands).

Command Modes

Exec > Global Configuration > APN Remap Table Configuration

configure > apn-remap-table table_name

Entering the above command sequence results in the following prompt:

[local]host_name{apn-remap-table_name}#

Important

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

- apn-remap, page 1837
- apn-selection-default, page 1840
- blank-apn, page 1844
- cc, page 1845
• description, page 1847
• end, page 1848
• exit, page 1849
• wildcard-apn, page 1850
apn-remap

Creates an entry in the APN remap table and provides the ability to override the APN requested by the UE.

Product

MME
SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > APN Remap Table Configuration

configure > apn-remap-table table_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-remap-table_name)#

Syntax Description

apn-remap { network-identifier apn_net_id { new-ni new_apn_net_id | operator-identifier apn_op_id new-ni new_apn_net_id { new-oi new_apn_op_id | value-for-oi-mcc mcc | value-for-oi-mnc mnc } | value-for-ni-wc new_apn_net_id } | operator-identifier apn_op_id { new-oi new_apn_op_id | value-for-oi-mcc mcc | value-for-oi-mnc mnc } }

no apn-remap { network-identifier apn_net_id | operator-identifier apn_op_id }

no

Deletes the specified APN remap entry from the APN remap table.

network-identifier apn_net_id

Identifies the "old" APN network identifier that is being mapped for replacement.

apn_net_id is a string of 1 to 62 characters, including digits, letters, dots (.) and dashes (-). Additionally, one wildcard character (*) can be included anywhere within the string.

new-ni new_apn_net_id

Identifies the new (target) network identifier to use when no wildcard character is included in the "old" APN network identifier.

new_apn_net_id is a string of 1 to 62 characters, including digits, letters, dots (.) and dashes (-).

value-for-ni-wc new_apn_net_id

Identifies the information to replace the wildcard in the new APN network identifier when a wildcard character is included in the "old" APN network identifier.
new_apn_net_id is an alphanumeric string of characters, including dots (.) and dashes (-). This string replaces the wildcard (*) specified in the apn_net_id. The two strings together must not exceed 62 characters.

**operator-identifier apn_op_id**

Identifies the "old" APN operator identifier that is being mapped for replacement.

*apn_op_id* is a string of 1 to 18 characters including digits, letters, and dots (.). The entry must be in the following format, where # represents a digit: MNC###.MCC###.GPRS.

Optionally, either one or two wildcard characters (*) can be entered. Wildcard characters can be used in place of one # or three # -- for example MNC12*.MCC*.GPRS.

**new-oi new_apn_op_id**

Identifies the new (target) operator identifier to use when no wildcard character is included in the "old" APN operator identifier.

*new_apn_op_id* is a string of 1 to 18 characters including digits, letters, and dots (.). The entry must be in the following format, where # represents a digit: MNC###.MCC###.GPRS.

**value-for-oi-mcc mcc**

Identifies the information to replace the wildcard in the new APN operator identifier when a wildcard character is included in the MCC portion of the "old" APN operator identifier; for example MNC###.MCC*.GPRS.

**value-for-oi-mnc mnc**

Identifies the information to replace the wildcard in the new APN operator identifier when a wildcard character is included in the MNC portion of the "old" APN operator identifier; for example MNC*.MCC###.GPRS.

---

**Usage Guidelines**

**Important**

Entries in the APN remap table are only valid if the table is associated with an operator policy. The same table can then be associated with an IMEI profile as IMEI-specific remap entries are not supported.

This command defines mapping entries in the APN remap table which supports a range of APN overrides. Mapping can be done one-to-one:

- a "new" APN network identifier (NI) can be mapped to override an "old" APN network identifier (NI) or an "old" APN operator identifier (OI)
- a "new" APN operator identifier (OI) can be mapped to override an "old" APN network identifier (NI) or an "old" APN operator identifier (OI)

Mapping can also be done with wildcards in the "old" APN entry mapped to wildcard replacements to dynamically create "new" APN network/operator identifiers.

**Related Commands:** APN override can also be based on charging characteristics. This type of override mapping is defined with the cc command, also part of this configuration mode.

**Examples**

A one-to-one APN NI remap entry is illustrated by:

```
apn-remap network-identifier 123abc.com new-ni 333CBC.com
```
Create an entry with a wildcard so that part of an incoming APN NI will be replaced - for example, incoming xyzabc$pqr.com becomes xyzinternet2$pqr.com.

```
apn-remap network-identifier xyz*pqr.com value-for-ni-wc internet2
```

Replace any incoming APN NI with a new APN NI.

```
apn-remap network-identifier * value-for-ni-wc newnet.com
```

A one-to-one APN OI remap entry is illustrated by:

```
apn-remap operator-identifier MNC423.MCC222.GPRS new-oi MNC123.MCC456.GPRS
```

Replace any incoming APN OI with a new APN OI MNC123.MCC456.GPRS:

```
apn-remap operator-identifier MNC*.MCC*.GPRS value-for-oi-mnc 123 value-for-oi-mcc 456
```
**apn-selection-default**

Enables and configures or disables the Default APN feature for use when the normal APN selection process fails.

**Product**
- MME
- SGSN

**Privilege**
- Security Administrator
- Administrator

**Command Modes**
- Exec > Global Configuration > APN Remap Table Configuration
- configure > apn-remap-table table_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-remap-table_name) #
```

**Syntax Description**

```
no apn-selection-default { first-in-subscription | lowest-context-id | network-identifier apn_net_id }
```

**no**
Delete the configuration statement and disable the default APN feature.

**first-in-subscription**

Specifies that the first APN in the subscription record matching the requested PDN type is used as the default APN. This applies when normal APN selection fails and if the UE APN is absent and the defined default APN is not a match.

For the SGSN, "first-in-subscription" means the first record from the list of records sent from the HLR (in the same order) with PDP type matching the requested PDP type. With this configuration, if the first record is a wildcard APN it is expected that the wildcard APN be configured. If not, the activation will be rejected.

For the MME, "first-in-subscription" means the first record from the list of records (apn-list) sent from the HSS with PDP type matching the UE-requested PDP type. The apn-list is sorted according to apn-name.

**lowest-context-id**

Specifies that the subscription APN with the lowest context-ID in the subscription record matching the PDN type is used as the default APN when normal APN selection fails.
With this configuration, if the record with the lowest context-ID is a wildcard APN, then it is expected that the wildcard APN has already been configured. If not, the activation will be rejected.

If both `apn-selection-default lowest-context-id` and `apn-selection-default first-in-subscription` options are configured, whichever command was executed (configured) first will be the behavior used.

Starting with Release 14.0, MME also supports use of this keyword.

**network-identifier `apn_net_id`**

Specifies the network identifier will be used as the default APN name as a string of 1 to 62 characters, including digits, letters, dots (.) and dashes (-).

Any of the following optional keywords can be used with `network-identifier` as qualifications.

**fallback-apn network-identifier `apn_net_id`**

SGSN only.

Specifies a dummy APN to be used when the default APN is not present in the subscription so that the activation does not fail. With this keyword configured, the context is activated with a dummy APN and the GGSN displays a static page for this APN, instructing the subscriber to subscribe for appropriate services.

`apn_net_id` is a string of 1 to 62 characters, including letters, digits, dots (.) and dashes (-).

**fallback-to-first-in-subscription**

Uses the APN from the first subscription record when the configured default APN is not available.

**prefer-single-subscription**

Uses the APN from the subscription record if it is the only record available and normal APN selection fails.

**reject-blank-apn**

Disables use of the default APN if a blank APN is received.

**require-dns-fail-wildcard**

Enables the default APN to be used if the DNS query fails with the requested APN.

Starting with Release 18.2, this keyword is also supported by the MME.

**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` is a string of 1 to 62 characters, including letters, digits, dots (.) and dashes (-).

**Usage Guidelines**

The default APN feature will be used in error situations when the MME or the SGSN cannot select a valid APN via the normal APN selection process. Within an operator policy, an APN remap table with a default APN can be configured for the MME/SGSN to:

- override a requested APN when the HSS/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.

The default APN feature can also be used in the event of a DNS query failure with the selected APN, if:

• the wildcard-apn command is configured, (requirement only for SGSN)
• a wildcard subscription is present,
• the require-dns-fail-wildcard keyword is included with the apn-selection-default command then the configured default APN will be used when the DNS query is retried.

In all of the instances outlined above, the MME/SGSN can provide the default APN as an alternate behavior to ensure that PDP context activation is successful.

**Important**

For SGSN ONLY - Beginning with Release 16, customers already using an APN remap table that is associated with an IMEI profile will have to change the existing configuration to enable the default APN remapping associated with an operator policy rather than the one associated with an IMEI profile. For example, if an existing configuration forced all matching IMEI in a defined IMEI range to use xxx.net APN, the configuration needs to be changed to an APN remap table configuration similar to what is shown below:

Old APN remap table associated with an IMEI profile:

```
apn-selection-default network-identifier xxx.net
```

For a configuration to accomplish the same remapping function, change the APN remap table associated with an IMEI profile to the following:

```
apn-remap network-identifier * new-ni xxx.net
```

**Important**

For SGSN ONLY - With Release 16, an APN remap table associated with an IMEI profile overrides a remap table associated with an operator policy. This means activation will be rejected if a local default APN configured, in an APN remap table associated with an IMEI profile, cannot be used. This will occur even if a valid local default APN is available in an APN remap table associated with an operator policy.

For SGSN ONLY - Beginning with Release 16, the following sample configuration will enable the operator to bypass APN remapping for a specific IMEI range:

```
config
  operator-policy name OpPol1
    associate call-control-profile OpPol1CCprof1
    associate apn-remap-table RemapOpPol1
    imei-range first start_imei last ending_imei | sv IMEI_sv | imei-profile name IMEIprof1
      exit
    imei-profile name IMEIprof1
      associate apn-remap-table remapIMEIprof1
      exit
  apn-remap-table remapIMEIprof1
    exit
  apn-remap-table RemapOpPol1
    apn-selection-default network-identifier NewAPN.net
end
```
Examples

The following command enables the default APN feature for APN HomeNet1 in an APN remap table associated with an operator policy:

```
apn-selection-default network-identifier HomeNet1
```

For SGSN only - Beginning with Release 16, if the APN remap table is associated with an IMEI profile, for a configuration to accomplish the same remapping function as noted in the sample above, then use syntax similar to the following:

```
apn-remap network-identifier * new-ni  xxx.net
```

The following command, in an APN remap table associated with an operator policy, enables use of a default APN selected on the basis of lowest context-ID if the APN is not contained within the subscription:

```
apn-selection-default lowest-context-id
```

The following command enables use of a default APN if the DNS query fails:

```
apn-selection-default network-identifier HomeNet1 require-dns-fail-wildcard
```
**blank-apn**

Enables the Blank APN feature and defines the APN that will be used when no APN is requested. This command is specific to SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Remap Table Configuration

configure > apn-remap-table table_name

Entering the above command sequence results in the following prompt:

[local] host_name (apn-remap-table_name) #

**Syntax Description**
blank-apn network-identifier apn_net_id
no blank-apn

**Usage Guidelines**
Use this command to enable the Blank APN feature.

**Examples**
The following command creates an entry that supplies the *starnet.com* as the APN network identifier whenever a request does not include an APN:

blank-apn network-identifier starnet.com
CC

This command maps an APN override based on charging characteristics.

Product

- MME
- SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > APN Remap Table Configuration

configure > apn-remap-table table_name

Entering the above command sequence results in the following prompt:

[local] host_name (apn-remap-table_name) #

Syntax Description

CC behavior bit_value profile index_bit apn-remap network-identifier apn_net_id new-ni new_apn_net_id

no CC behavior bit_value profile index_bit apn-remap network-identifier apn_net_id

no

Disables the configured cc-based remapping behavior.

behavior bit_value

Specifies the value for the charging characteristic behavior bit.

bit_value is a hex value from 0x0 to 0xFFF.

profile index_bit

Specifies the index for the charging characteristic profile.

index_bit is an integer from 1 through 15.

Some of the index values are predefined according to 3GPP standards:

- 1 for hot billing
- 2 for flat billing
- 4 for prepaid billing
- 8 for normal billing
**apn-remap network-identifier apn_net_id**

Identifies the "old" APN network identifier that is being mapped for replacement.

*apn_net_id* is a string of 1 to 62 characters, including letters, digits, dots (.) and dashes (-).

**new-ni new_apn_net_id**

Identifies the "new" APN network identifier that is being mapped to.

*new_apn_net_id* is a string of 1 to 62 characters, including letters, digits, dots (.) and dashes (-).

**Usage Guidelines**

Use this command to enable APN remapping only when the charging characteristic value in the subscription record associated with the requested APN matches the value configured for the **new-ni**.

The new APN NI must be part of the subscription data so that the charging characteristic associated with the new APN NI will be used for activating the context. If there is not one associated, then the general charging characteristic will be used.

**Examples**

The following command associates a new APN NI *locals1* with a set of charging characteristics:

```
cm behavior 0xF profile 4 apn-remap network-identifier homer1 new-ni locals1
```
**APN Remap Table Configuration Mode**

**description**

Defines a string that describes this APN remap table.

**Product**

MME

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Remap Table Configuration

```
configure > apn-remap-table table_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (apn-remap-table_name) #
```

**Syntax Description**

```
description description

no description

no
```

Removes the description configuration from this APN Remap Table configuration.

```
description
```

Specifies descriptive text to be associated with the APN remap table as an alphanumeric string of 1 through 100 characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotation marks (").

**Usage Guidelines**

Define information that identifies this particularly APN remap table.

**Examples**

```
description "APN_remap1 replaces all MNC1## Ids."
```
end

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

Product     All

Privilege    Security Administrator, Administrator

Syntax Description     end

Usage Guidelines     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 Description**
exit

**Usage Guidelines**
Use this command to return to the parent configuration mode.
**wildcard-apn**

Enables or disables the Wildcard APN feature and define the default APN to be used whenever a wildcard APN is included in the subscriber record.

**Product**

MME  
SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Remap Table Configuration  
**configure > apn-remap-table table_name**

Entering the above command sequence results in the following prompt:

```
[local] host_name(apn-remap-table_name)#
```

**Syntax Description**

```wildcard-apn pdp-type { dual-ipv4v6 | ipv4 | ipv6 | ppp } network-identifier apn_net_id```

no wildcard-apn pdp-type { dual-ipv4v6 | ipv4 | ipv6 | ppp }

no

Disables the wildcard-apn definition from the configuration.

**pdp-type {dual-ipv4v6 | ipv4 | ipv6 | ppp }**

Specifies the PDP type.

- **dual-ipv4v6** - for a dual PDP context association with one IPv4 address and one IPv6 address/prefix (SGSN only)
- **ipv4** - for an IPv4 context
- **ipv6** - for an IPv6 context
- **ppp** - for a PPP context

**network-identifier apn_net_id**

Identifies one of the APN network identifiers specified via the **apn** command in the Operator Policy configuration mode.

*apn_net_id* is a string of 1 to 62 characters, including letters, digits, dots (.) and dashes (-).
**Usage Guidelines**

This command is used to define a wildcard APN with the type of PDP context and the APN's network identifier (NI). This wildcard APN would be used when an APN is not identified.

The command should be repeated per PDP type, as needed, to enable wildcard APN for two or more of the PDP types.

The wildcard APN configured with the dual PDP IPv4v6 context will be used in the following scenarios:

- the UE requested a PDP type of IPv4v6
- the UE did not request any specific APN
- the subscription includes wildcard APN with PDP type as IPv4v6.

---

**Important**

Wildcard APN feature configuration is only valid if the APN remap table is associated with at least one operator policy. The same table can then be associated with an IMEI profile as IMEI-specific Wildcard APN is not supported.

---

**Examples**

Use this command to enable an APN wildcard for PDP type IPv4 and NI `homer1`:

```
wildcard-apn pdp-type ipv4 network-identifier homer1
```
wildcard-apn
ARP-RP Mapping Profile Configuration Mode

The SGSN uses the ARP to RP mapping for a variety of reasons, such as choosing a preferred radio priority according to the ARP values sent by the GGSN and HLR. These mappings will be used by corresponding 2G and/or 3G services to choose the radio priority value sent in downlink messages towards the MS/UE:

- Activate PDP Accept.
- Modify PDP Request during network-initiated PDP modification procedure.
- Modify PDP Accept during MS-initiated PDP modification procedure provided the ARP has been changed by the network.

The commands in this mode configure the various parameters of the ARP-RP Mapping Profile.

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration > ARP-RP Mapping Profile Configuration

`configure > sgsn-global > qos-arp-rp-map-profile arp-rp_prof_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-arp-rp-map-profile-arp-rp_prof_name)#
```

**Important**

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

```
- arp, page 1854
- end, page 1856
- exit, page 1857
```
arp

This command modifies the ARP (allocation retention priority) to RP (radio priority) mapping in the ARP-RP Mapping Profile.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration > ARP-RP Mapping Profile Configuration

```
configure > sgsn-global > qos-arp-rp-map-profile arp-rp_prof_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-arp-rp-map-profile-arp-rp_prof_name) #
```

**Syntax Description**

```
arp  arp_value radio-priority rp_value
```

*arp*

Defines the allocation retention priority.

*arp_value*: Enter an integer from 1 to 3.

*radio-priority*

Defines the radio priority.

*rp_value*: Enter an integer from 1 to 4.

**Usage Guidelines**

When the ARP-RP Mapping Profile is created it includes default ARP-RP mapping:

- ARP1 RP4
- ARP2 RP4
- ARP3 RP4

The commands in this mode can be issued as needed to modify the mapping.

Use the `show sgsn-mode` command to display the ARP-RP profile and configuration.

Use the `radio-priority` keyword of the `sm` command in either the GPRS Service configuration mode or the SGSN Service configuration mode to associate the ARP-RP Mapping Profile with either of the service types.
Examples

To change the radio priority from 4 to 2 for the allocation retention priority of 1, use the following command.

```
arp 1 rp 2
```
**end**

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

end

**Usage Guidelines**

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 Description**
exit

**Usage Guidelines**
Use this command to return to the parent configuration mode.
exit
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.

**Command Modes**

Exec > Global Configuration > ATM Port Configuration

*configure* > *port atm* *slot_number/port_number*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-port-slot_number/port_number) #
```

**Important**

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

- clock-source, page 1861
- description, page 1862
- end, page 1863
- exit, page 1864
- line-timing, page 1865
- loopback, page 1866
- preferred slot, page 1868
- pvc, page 1870
- shutdown, page 1872
- snmp trap link-status, page 1873
- threshold high-activity, page 1874
- threshold monitoring, page 1876
- threshold rx-utilization, page 1878
- threshold tx-utilization, page 1880
- toh-sdsf, page 1882
**clock-source**

This command sets the source of the port's transmit clock.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > ATM Port Configuration

```
configure > port atm slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-port-slot_number/port_number)#
```

**Syntax Description**

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 Guidelines**

Use this command for either SONET ports on the SGSN.

**Important**

This command is only available for releases 8.1 or higher.

**Examples**

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

**Command Modes**

Exec > Global Configuration > ATM Port Configuration

`configure > port atm slot_number/port_number`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax Description**

- `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 Guidelines**

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.

**Examples**

The following example sets a port description that will read in the configuration file:

```
description samplePortDescriptiveText
```

The following example sets a port description that will be easy to read because it retains the spaces between words:

```
description "This is a sample description"
```
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

dend

Usage Guidelines

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 Description**

exit

**Usage Guidelines**

Use this command to return to the parent configuration mode.
line-timing

This command enables the SPIO to recover transmit timing source via the line attached to the selected port. By default, line-timing is not enabled.

To employ line-timing recovery, the SPIO card(s) must be equipped with the optional Stratum 3 clock module.

Important

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > ATM Port Configuration

configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax Description

| no | line-timing

no

Disables line-timing as the source for the transmit clock.

Usage Guidelines

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 in the BITS port configuration mode.

Important

If the SPIO is connected to an external Building Integrated Timing Supply (BITS) source, BITS timing always takes precedence over line-timing.

Examples

Disable configured line-timing as the clock source for this port.

no line-timing
loopback

Enables/disables loopback and configures the type of loopback mode used for diagnostic testing.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > ATM Port Configuration
configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:
[local] host_name (config-port-slot_number/port_number) #

**Syntax Description**

```plaintext
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 Guidelines**
Setup diagnostic loopback signals for troubleshooting purposes.

**Examples**
Use the following command to setup loopback diagnosis:

```
loopback ds1-e1-diag
```
Use the following command to disable loopback:

```
loopback none
```
preferred slot

This command identifies which card in a chassis assumes revertive (redundancy auto-recovery) functionality when the slot/port being configured go down.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ATM Port Configuration
configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:
[local] host_name(config-port-slot_number/port_number) #

Syntax Description

preferred slot slot#
 [ default | no ] preferred slot

default

Default: non-revertive operation.
Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a port switch command to return service to the original port.

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 Guidelines

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.

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.

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.
Examples

The following commands sets revertive port redundancy for ports on the card in slot 17:

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.

---

**Important**

In Release 20.0, HNB-GW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

---

**Product**

HNB-GW

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > ATM Port Configuration

`configure > port atm slot_number/port_number`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-port-slot_number/port_number)#
```

**Syntax Description**

```
[ no ] pvc vpi vpi# vci vci# [ type { aal2 [ cps-payload-size cps_payload_value | aal5 ] } ] | -noconfirm |
```

- **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.

- **type**
  This keyword is used to define the type of PVC as AAL2 or AAL5 for HNB-GW service configuration within the associated VPI and VCI.
**aal2**

This keyword is used to define the type of PVC as AAL2 for HNB-GW service configuration within the associated VPI and VCI.

**aal5**

This keyword is used to define the type of PVC as AAL5 for HNB-GW service configuration within the associated VPI and VCI.

**cps-payload-size cps_payload_value**

This keyword configures the Common Part Sublayer (CPS) payload in Bytes for AAL2 type of PVC within the associated VPI. CPS payload is carried out by the AAL2 protocol over ATM. During the call, the payload size is negotiated between HNB-GW and MSC. Default size for payload is 64 but values may range from 1 to 64 Bytes. This command makes the operator to choose the size dynamically.

The CPS payload size dynamically configured for per PVC. If user is not providing the CPS payload size then default value of 64 Bytes is considered else user provided value is taken.

**-noconfirm**

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

---

**Usage Guidelines**

Creates a virtual circuit between two specific points that the carrier will use repeatedly.

This command is used to define the type of PVC as AAL2 or AAL5 for HNB-GW service configuration. It also configures the CPS payload which is carried out by the AAL2 protocol over ATM. During the call, the payload size is negotiated between HNB-GW and MSC. Default size for payload is 64 but values may range from 1 to 64 Bytes. This command makes the operator to choose the size dynamically.

This command configures the type of PVC to ATM Adaptation Layer2 (AAL2) or ATM Adaptation Layer5 (AAL5) for ATM traffic between HNB-GW and MSC. It also enables the operator to configure the Common Part Sublayer (CPS) payload for AAL2 protocol over ATM for HNB-GW session between MSC and HNB-GW.

**Examples**

Define a PVC with VPI 2 and VCI 353.

```
pvc vpi 2 vci 353
```

The following command configures the PVC type as AAL2 with VPI as 2 and VCI as 353. It also configures the CPS payload to 45 bytes over the ATM during the call.

```
pvc vpi 2 vci 353 type aal2 cps-payload-size 45
```
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

Command Modes

Exec > Global Configuration > ATM Port Configuration
configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:

[local] host_name(config-port-slot_number/port_number)#

Syntax Description

| no | shutdown

no

Enables the port's administrative state. When this command is omitted from the configuration, the card is shutdown (removed from service).

Usage Guidelines

Shut down a port prior to re-cabling and/or other maintenance activities. This is the default state of each port upon installation and initial configuration.

This command with the no keyword is required to bring a port into active service.

Examples

The following command enables the port for service:

no shutdown

The following command disables the port and takes it out of service:

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

Command Modes

Exec > Global Configuration > ATM Port Configuration
configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:

[local] host_name (config-port-slot_number/port_number)#

Syntax Description

| no | snmp trap link-status

no

Disables the sending of traps for link-status changes.

Usage Guidelines

Enable the sending of link-status change traps for this port if there is a monitoring facility that can use the information or if there are troubleshooting activities in progress.

Examples

Use the following command to send SNMP link-status traps for this port:

snmp trap link-status

Use the following command to disable the sending SNMP link-status traps for this port:

no snmp trap link-status
threshold high-activity

Configures the port's high and low activity thresholds.

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > ATM Port Configuration

configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:
[local] host_name (config-port-slot_number/port_number) #

Syntax Description

threshold high-activity high_thresh [ clear low_thresh ]
default threshold high-activity

default
Restores both port high-activity thresholds to the system default of 50 percent.

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 Guidelines

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.

Examples

The following command configures a high port utilization threshold of 70 percent and a low threshold of 50 percent for a system using the Alarm thresholding model:

```
threshold high-activity 70 clear 50
```
threshold monitoring

Enables thresholding for port-level values.

Important

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Product

HNB-GW
SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ATM Port Configuration
configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:
[local]host_name(config-port-slot_number/port_number)#

Syntax Description

| default | no | threshold monitoring |

default

Restores the system default to disable threshold monitoring for port-level values.

no

Disables threshold monitoring for port-level values. This is the default setting.

Usage Guidelines

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 20: 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></td>
<td>X</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 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.

Important
In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Product
HNB-GW
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > ATM Port Configuration
configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:
[local]host_name(config-port-slot_number/port_number)#

Syntax Description

threshold rx-utilization high_thresh [ clear low_thresh ]
default threshold rx-utilization

default
Restores both rx-utilization thresholds to the system default of 80 percent.

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 Guidelines**

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.

**Examples**

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.

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Product

HNB-GW
SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ATM Port Configuration
configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:

[local] host_name(config-port-slot_number/port_number)#

Syntax Description

threshold tx-utilization high_thresh [ clear low_thresh ]
default threshold tx-utilization

default
Restores the port tx-thresholds to their system defaults of 80 percent.

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 Guidelines

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.

Examples

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**

Enable/disable line SDSF BER thresholds and configure the line transport overhead (TOH) signal degrade and signal failure (SDSF) bit error rate (BER) threshold.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > ATM Port Configuration

configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:

[local] host_name(config-port-slot_number/port_number)#

**Syntax Description**

`toh-sdsf toh_value`

`default toh-sdsf`

**default**

Resets the default which disables this threshold.

`toh_value`

To facilitate configuration the SD and SF rates have been combined into a single setting.

- 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 Guidelines  
This command is typically configured in combination with configuring APS/MSP redundancy for the line card - see the `aps` and the `redundancy` commands documented in the `Card Configuration Mode Commands` chapter.

This command can be used to configure the line threshold whether the port is active or standby and sets a standard option for the paired values of the line's signal degrade and signal failure (SDSF) BER.

The SD is kept at a value of 100 erroredBits/sec less than the corresponding value of the SF. So if the SD threshold is configured at 1 error in every 100000 bits/sec, then the SF threshold automatically becomes 1 error in every 1000 bits/sec.

The port will go operationally down as soon as the SD threshold is crossed.

Examples  
Set the SD and SF rates to 1.E-04:
```
toh-sdsf 1
```
Bearer Control Profile Configuration Mode Commands

The Bearer Control Profile configuration mode provides the commands to define the MME's bearer-level QoS control parameters. Bearer-level parameters such as ARP, MBR, GBR, QCI remap value can be configured independently for either or both default/dedicated bearers along with the capping action, such as prefer-as-cap or pgw-upgrade, in bearer control profile. The bearer control profile can be applied for a specific QCI or a range of QCIs.

The bearer control profile becomes valid after it is associated with an MME QoS profile.

Command Modes

Exec > Global Configuration > Bearer Control Profile Configuration

catalog > bearer-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(bearer-control-profile-be_profile_name)#

Important

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

- dedicated-bearer, page 1886
- default-bearer, page 1890
- description, page 1894
- end, page 1895
- exit, page 1896
- pre-rel8-qos-mapping, page 1897
dedicated-bearer

Use this command to define the operator-provided values for ARP-PL, ARP-PCI, ARP-PVI, MBR, GBR, and QCI, as well as pgw-upgrade capping.

**Product**  MME

**Privilege**  Administrator

**Command Modes**  Exec > Global Configuration > Bearer Control Profile Configuration

`configure > bearer-control-profile profile_name`

Entering the above command sequence results in the following prompt:

`[local] host_name(bearer-control-profile-bc_profile_name)#`

**Syntax Description**

```
dedicated-bearer  { arp  preemption-capability  preemption-vulnerability  priority-level  } pgw-upgrade  { local  minimum  rej-if-exceed  } gbr gbr-up gbr-up_value  gbr-down gbr-down_value  pgw-upgrade  { local  minimum  rej-if-exceed  } mbr mbr-up mbr-up_value  mbr-down mbr-down_value  pgw-upgrade  qci  remap  pgw-upgrade  { local  minimum  rej-if-exceed  }  }
```

`remove dedicated-bearer  { arp  gbr  mbr  qci  }`

**remove**

Including this command prefix causes the MME to delete the dedicated-bearer configuration for the named bearer control profile.

**arp**

This keyword configures the allocation and retention priority parameters:

- **preemption-capability** - Enter an integer, either 0 (may) to specify that this bearer may pre-empt other lower priority bearers if required, or 1 (shall-not) to specify that this bearer shall not pre-empt other lower priority bearers.

- **preemption-vulnerability** - Enter an integer, either 0 (pre-emptible) to specify that this bearer is pre-emptible by other high priority bearers, or 1 (not-pre-emptible) to specify that this bearer is not pre-emptible by other high priority bearers.

- **priority-level** - Enter an integer 1 through 15, with 1 as the highest priority, to specify the allocation/retention priority level.
**gbr**

The **gbr** keyword configures the Guaranteed Bit Rate values. This keyword is only used for the dedicated-bearer configuration.

- **gbr-up** - Enter an integer from 1 though 256000 to identify the desired uplink data rate in kbps.
- **gbr-down** - Enter an integer from 1 though 256000 to identify the desired downlink data rate in kbps.

**mbr**

The **mbr** keyword configures the Maximum Bit Rate values. This keyword is only used for the dedicated-bearer configuration.

- **mbr-up** - Enter an integer from 1 though 256000 to identify the desired uplink data rate in kbps.
- **mbr-down** - Enter an integer from 1 though 256000 to identify the desired downlink data rate in kbps.

**qci remap**

The **qci remap** keyword sets the locally configured QCI. Enter an integer from 1 through 9. The QCI remap mechanism maps an incoming QCI or a range of QCI to the configured QCI or range of QCI. QCI remap is the first configuration that is applied, from the bearer control profile configuration, and it is applicable only during Create Session Request and Create Bearer Request procedures. The Bearer Control profile associated to the remapped QCI value is used for capping the remaining QoS parameters.

**pgw-upgrade**

The **pgw-upgrade** keyword can be included with any of the other keywords. It identifies the capping mechanism to be used when QoS parameters are received from the PGW and the options include:

- **local** - Instructs the MME to select locally configured values for QoS capping.
- **minimum** - Instructs the MME to select the lower value, of the two values locally configured or received value, to use as the QoS capping value.
- **rej-if-exceed** - Instructs the MME to reject the call if the received value exceeds the locally configured value.

**Usage Guidelines**

Repeat the **dedicated-bearer** command as needed to configure all parameters of interest.

**QoS Computation** - The following explains how the resultant QoS values are derived for the **minimum** and **reject-if-exceed** actions configured under **pgw-upgrade**.

- **QCI**

  - Every standard GBR/non-GBR QCI is associated with a priority level as per 3GPP TS 23.203 v12.10.0, Table 6.1.7.

<table>
<thead>
<tr>
<th>QCI</th>
<th>Resource Type</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GBR</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>GBR</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>GBR</td>
<td>3</td>
</tr>
</tbody>
</table>
**Priority Resource Type QCI**

<table>
<thead>
<tr>
<th>QCI</th>
<th>Resource Type</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>GBR</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>non-GBR</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>non-GBR</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>non-GBR</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>non-GBR</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>non-GBR</td>
<td>9</td>
</tr>
</tbody>
</table>

- Priority Level 1 has the highest priority and in case of congestion lowest priority level traffic would be the first to be discarded.
- **minimum**: The QCI with lower priority level will be used.
- **rej-if-exceed**: If the received QCI has higher priority level than the configured local QCI, then the procedure will be rejected.

**・ARP Priority Level**

- ARP Priority level decreases on increasing value (1 to 15). ARP Priority level 1 has the highest priority value.
- **minimum**: The lower ARP Priority level (i.e. higher value) will be used.
- **rej-if-exceed**: If the received ARP Priority level is higher (i.e. value is lesser) than the CLI configured local ARP Priority level, then the procedure will be rejected.

**・ARP-PCI**

- Preemption capability indicator can have either of the following two values, where may (0) > shall-not (1)
  - **may** - specifies that this bearer may preempt other lower priority bearers, if required
  - **shall-not** - specifies that this bearer shall-not pre-empt other lower priority bearers.

*Following table indicates the resultant pre-emption capability for the minimum pgw-upgrade*

<table>
<thead>
<tr>
<th>Received value</th>
<th>Configured local value</th>
<th>Resultant value to be used</th>
</tr>
</thead>
<tbody>
<tr>
<td>may</td>
<td>may</td>
<td>may</td>
</tr>
<tr>
<td>may</td>
<td>shall-not</td>
<td>shall-not</td>
</tr>
<tr>
<td>shall-not</td>
<td>may</td>
<td>shall-not</td>
</tr>
<tr>
<td>shall-not</td>
<td>shall-not</td>
<td>shall-not</td>
</tr>
</tbody>
</table>

- **rej-if-exceed**: If the received ARP-PCI value is **may** and the configured local value is **shall-not**, then the procedure will be rejected.
• Default value set by MME if not provided by HSS/PGW: shall-not

• ARP-PVI

• Preemption vulnerability indicator can have either of the following two values, where not-pre-emptible (1) > pre-emptible (0)

  * pre-emptible - specifies that this bearer is pre-emptible by other high priority bearers
  * not-pre-emptible - specifies that this bearer is NOT pre-emptible by other high priority bearers

• Following table indicates the resultant pre-emption vulnerability for the minimum pgw-upgrade:

<table>
<thead>
<tr>
<th>Received value</th>
<th>Configured local value</th>
<th>Resultant value to be used</th>
</tr>
</thead>
<tbody>
<tr>
<td>pre-emptible</td>
<td>pre-emptible</td>
<td>pre-emptible</td>
</tr>
<tr>
<td>pre-emptible</td>
<td>not-pre-emptible</td>
<td>pre-emptible</td>
</tr>
<tr>
<td>not-pre-emptible</td>
<td>pre-emptible</td>
<td>pre-emptible</td>
</tr>
<tr>
<td>not-pre-emptible</td>
<td>not-pre-emptible</td>
<td>not-pre-emptible</td>
</tr>
</tbody>
</table>

• rej-if-exceed: If the received ARP-PVI value is not-pre-emptible and the configured local value is pre-emptible, then the procedure will be rejected.

• Default value set by the MME if not provided by the HSS/PGW: pre-emptible

• MBR / GBR

• minimum:

  * Uplink - The lower of the values, comparing the received values and the configured local value, will be used for APN-AMBR/MBR/GBR.
  * Downlink - The lower value of the received value and configured local value will be used for APN-AMBR/MBR/GBR.

• rej-if-exceed: If the received Uplink value is greater than the configured local Uplink value or the received Downlink value is greater than the configured local Downlink value, then the procedure will be rejected.

**Examples**

The following is a sample command to configure ARP capping for dedicated bearers:

`dedicated-bearer arp priority 1 pgw-upgrade local`

The following is a sample command to configure MBR capping for dedicated bearers:

`dedicated-bearer mbr max-ul 20000 max-dl 20000 pgw-upgrade minimum`
default-bearer

Use this command to configure the operator-provided values for the ARP and QCI QoS control parameters, as well as the prefer-as-cap and pgw-upgrade capping.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Bearer Control Profile Configuration

`configure > bearer-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name (bearer-control-profile--bc_profile_name)#
```

**Syntax Description**

```
default-bearer { arp { { preemption-capability | preemption-vulnerability | priority-level } { pgw-upgrade | prefer-as-cap } { local | minimum | rej-if-exceed } } | qci { remap | pgw-upgrade { local | minimum | rej-if-exceed } } }
remove default-bearer { arp | qci }
```

remove

Including this command prefix instructs the MME to delete the default-bearer configuration.

**arp**

This keyword configures the allocation and retention priority parameters:

- **preemption-capability** - Enter an integer, either 0 (may) to specify that this bearer may pre-empt other lower priority bearers if required, or 1 (shall-not) to specify that this bearer shall not pre-empt other lower priority bearers.

- **preemption-vulnerability** - Enter an integer, either 0 (pre-emptible) to specify that this bearer is preemptible by other high priority bearers, or 1 (not-pre-emptible) to specify that this bearer is not pre-emptible by other high priority bearers.

- **priority-level** - Enter an integer 1 through 15, with 1 as the highest priority, to specify the allocation/retention priority level.

**pgw-upgrade**

The `pgw-upgrade` keyword can be included with any of the other keywords. It identifies the capping mechanism to be used when QoS parameters are received from the PGW and the options include:
• **local** - Instructs the MME to select locally configured values for QoS capping.

• **minimum** - Instructs the MME to select the lower value, of the two values locally configured or received value, to use as the QoS capping value.

• **rej-if-exceed** - Instructs the MME to reject the call if the received value exceeds the locally configured value.

**prefer-as-cap**

The *prefer-as-cap* keyword can be included with any of the other keywords. It identifies the capping mechanism to be used when QoS parameters are received from the HSS or from the peer-MME/S4-SGSN:

• **local** - The configured local value will be used.

• **minimum** - The minimum (lowest) value of the configured local value or the HSS-provided value will be used.

• **reject-if-exceed** - The request/procedure is rejected if the HSS-provided value exceeds the configured local value.

**qci remap**

The *qci remap* keyword sets the locally configured QCI. Enter an integer from 1 through 9. The QCI remap mechanism maps an incoming QCI or a range of QCI to the configured QCI or range of QCI. QCI remap is the first configuration that is applied, from the bearer control profile configuration, and it is applicable only during Create Session Request and Create Bearer Request procedures. The Bearer Control profile associated to the remapped QCI value is used for capping the remaining QoS parameters.

**Usage Guidelines**

Repeat the *default-bearer* command as needed to configure all parameters of interest.

**QoS Computation** - The following explains how the resultant QoS values are derived for the *minimum* and *reject-if-exceed* actions configured under *prefer-as-cap* or *pgw-upgrade*.

• **QCI**

Every standard GBR/non-GBR QCI is associated with a priority level as per 3GPP TS 23.203 v12.10.0, Table 6.1.7.

<table>
<thead>
<tr>
<th>QCI</th>
<th>Resource Type</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GBR</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>GBR</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>GBR</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>GBR</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>non-GBR</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>non-GBR</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>non-GBR</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>non-GBR</td>
<td>8</td>
</tr>
</tbody>
</table>
Priority Resource Type QCI

9 non-GBR 9

- Priority Level 1 has the highest priority and in case of congestion lowest priority level traffic would be the first to be discarded.

- **minimum**: The QCI with lower priority level will be used.

- **rej-if-exceed**: If the received QCI has higher priority level than the configured local QCI, then the procedure will be rejected.

- **ARP Priority Level**

  - ARP Priority level decreases on increasing value (1 to 15). ARP Priority level 1 has the highest priority value.

  - **minimum**: The lower ARP Priority level (i.e. higher value) will be used.

  - **rej-if-exceed**: If the received ARP Priority level is higher (i.e. value is lesser) than the CLI configured local ARP Priority level, then the procedure will be rejected.

- **ARP-PCI**

  - Preemption capability indicator can have either of the following two values, where may (0) > shall-not (1)

    - *may* - specifies that this bearer may preempt other lower priority bearers, if required

    - *shall-not* - specifies that this bearer shall-not pre-empt other lower priority bearers.

  - Following table indicates the resultant pre-emption capability for the *minimum* prefer-as-cap or pgw-upgrade

<table>
<thead>
<tr>
<th>Received value</th>
<th>Configured local value</th>
<th>Resultant value to be used</th>
</tr>
</thead>
<tbody>
<tr>
<td>may</td>
<td>may</td>
<td>may</td>
</tr>
<tr>
<td>may</td>
<td>shall-not</td>
<td>shall-not</td>
</tr>
<tr>
<td>shall-not</td>
<td>may</td>
<td>shall-not</td>
</tr>
<tr>
<td>shall-not</td>
<td>shall-not</td>
<td>shall-not</td>
</tr>
</tbody>
</table>

  - **rej-if-exceed**: If the received ARP-PCI value is *may* and the configured local value is *shall-not*, then the procedure will be rejected.

  - Default value set by MME if not provided by HSS/PGW: *shall-not*

- **ARP-PVI**

  - Preemption vulnerability indicator can have either of the following two values, where not-pre-emptible (1) > pre-emptible (0)

    - *pre-emptible* - specifies that this bearer is pre-emptible by other high priority bearers
*not-pre-emptible* - specifies that this bearer is NOT pre-emptible by other high priority bearers

Following table indicates the resultant pre-emption vulnerability for the *minimum* prefer-as-cap or pgw-upgrade:

<table>
<thead>
<tr>
<th>Received value</th>
<th>Configured local value</th>
<th>Resultant value to be used</th>
</tr>
</thead>
<tbody>
<tr>
<td>pre-emptible</td>
<td>pre-emptible</td>
<td>pre-emptible</td>
</tr>
<tr>
<td>pre-emptible</td>
<td>not-pre-emptible</td>
<td>pre-emptible</td>
</tr>
<tr>
<td>not-pre-emptible</td>
<td>pre-emptible</td>
<td>pre-emptible</td>
</tr>
<tr>
<td>not-pre-emptible</td>
<td>not-pre-emptible</td>
<td>not-pre-emptible</td>
</tr>
</tbody>
</table>

*rej-if-exceed:* If the received ARP-PVI value is *not-pre-emptible* and the configured local value is *pre-emptible*, then the procedure will be rejected.

*Default value set by the MME if not provided by the HSS/PGW: pre-emptible*

**Examples**

The following is an example of a command to configure QCI mapping for the default bearer:

default-bearer qci remap 6
description

Allows you to enter descriptive text for this configuration.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description
description text
no description

text

Enter descriptive text as an alphanumeric string of 1 to 100 characters.

If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

Usage Guidelines

The description should provide useful information about this configuration.
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

dend

Usage Guidelines

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 Description
exit

Usage Guidelines
Use this command to return to the parent configuration mode.
**pre-rel8-qos-mapping**

This command defines mapping of EPC QOS (non-standard QCIs) to 3GPP PreRelease8 QoS parameters in the MME.

**Product**  
MME

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Bearer Control Profile Configuration

```bash
configure > bearer-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name>(bearer-control-profile-bc_profile_name)#
```

**Syntax Description**

```
| remove | { pre-rel8-qos-mapping { class { background | conversational | interactive | streaming } } { thp thp_value } { sig-ind indicator_value } { src-stat-desc value } { min-transfer-delay value } { sdu error-ratio value } } | qci value |
```

- **remove**
  
  Including this command prefix causes the MME to delete the PreRelease8QoS parameter configuration for the named bearer control profile.

- **qci**
  
  qci indicates the QoS class. Its value ranges from 1 to 9. When QCI is configured, the corresponding mapping takes place based on 3GPP TS 23.401.

- **class**
  
  Indicates the UMTS traffic classified into the following categories:

  - **background**
  
  - **conversational**
  
  - **interactive**
  
  - **streaming**
thp
Traffic handling priority specifies the relative importance of handling all SDUs that belong to the UMTS bearer compared to the SDUs of other bearers. The priority value ranges from 1 to 3, where the value 1 holds the highest priority.

sig-ind
The sig-ind keyword toggles the state of the signal. The values are either 0 or 1.

src-stat-desc
The src-stat-desc (Source Statistics Descriptor) keyword toggles the state of the signal. The values are either 0 or 1.

sdu error-ratio
The Service Data Unit (SDU) Error ratio indicates the fraction of SDUs lost or detected as error packets. SDU error ratio is defined only for conforming traffic.

min-transfer-delay
The min-transfer-delay defines the maximum delay for 95th percentile of the delay distributed for all delivered SDUs during the lifetime of a bearer service. The delay value ranges from 10 to 40,000 milliseconds.

Usage Guidelines
An operator specific QCI can be remapped to another QCI using the Bearer Control Profile Configuration mode. Bearer level parameters such as ARP, MBR, GBR values can be configured independently for default/dedicated bearer along with actions such as prefer-as-cap or pgw-upgrade in the Bearer Control Profile Configuration mode.

The operator specific QCIs from 128 to 254 has the lowest priority. These priority values are considered while deriving resultant QoS values for the minimum and reject-if-exceed actions configured under prefer-as-cap or pgw-upgrade.

Examples
The following is a sample command to configure PreRelease8QoS parameter for the conversational class:
pre-rel8-qos-mapping class conversational thp 1 sig-ind 0 src-stat-desc 1 min-transfer-delay 100 sdu error-ratio 4

The following is a sample command to configure PreRelease8QoS parameter for the conversational class:
pre-rel8-qos-mapping class interactive thp 2 sig-ind 0 src-stat-desc 1 min-transfer-delay 300 sdu error-ratio 4
BFD Configuration Mode Commands

BFD provides a low-overhead, short duration method of detecting failures in the forwarding path between two BGP or OSPF adjacent routers, including the interfaces, data links, and forwarding plane. BFD must be enabled on both routers. The ASR 5000 and ASR 5500 supports BFD on Layer 3 clients only in asynchronous mode with optional Echo functionality.

The BFD Configuration Mode manages the protocol settings for Bidirectional Forwarding Detection (BFD).

**Command Modes**

```
Exec > Global Configuration > Context Configuration > BFD Configuration
```

```
configure > context context_name > bfd-protocol
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bfd) #
```

**Important**

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

**Important**

On the ASR 5000, one of the packet processing cards must be configured as a demux card for BFD to function.

- bfd linkagg-peer, page 1900
- bfd multihop-peer, page 1902
- bfd nbr-group-name, page 1904
- echo, page 1906
- end, page 1907
- exit, page 1908
- slow-timers, page 1909
**bfd linkagg-peer**

Enables member-link based BFD and configures the BFD link aggregation (linkagg) session values. Member-link based BFD detects individual link failures faster than LACP and reduces the overall session/traffic down period as a result of single member link failure.

**Product**

ASR 5000, ASR 5500 all products

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BFD Configuration

configure > context context_name > bfd-protocol

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-bfd)#
```

**Syntax Description**

```
bfd linkagg-peer linkagg_group_id local-endpt-addr local_endpt_ipaddress remote-endpt-addr remote_endpt_ipaddress interval tx_interval min_rx rx_interval multiplier multiplier_value | slot slot_number |
```

*no bfd linkagg-peer linkagg_group_id | slot slot_number |

*no*

Disables this member-link BFD configuration.

*linkagg_group_id*

Specifies the LAG number as an integer from 1 through 255.

*local-endpt-addr local_endpt_ipaddress*

Specifies the source address of the multihop BFD session in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal format.

*remote-endpt-addr remote_endpt_ipaddress*

Specifies the remote address of the Multihop BFD session in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal format.

*interval tx_interval*

Specifies the transmit interval of control packets in milliseconds as an integer from 50 through 10000.
**min_rx rx_interval**
Specifies the minimum receive interval for control packets in milliseconds as an integer from 50 through 10000.

**multiplier multiplier_value**
Specifies the value used to compute hold-down time as an integer from 3 through 50.

**slot slot_number**
For a redundant active-standby linkagg configuration, this option specifies the card for which this configuration is intended.

**Usage Guidelines**
Use this command to enable member-link based BFD and configures the BFD link aggregation session values (RFC 7130). Member-link based BFD detects individual link failures faster than LACP and reduces the overall session traffic down period as a result of single member link failure.

This command configures BFD interactions with the linkagg task. Once a session is configured, BFD creates per member link BFD sessions and starts sending packets on each of the linkagg member links. If a member link BFD session fails, StarOS notifies failures to the linkagg task.

If you define a linkagg-peer using a slot number, you may configure a linkagg-peer for the redundant slot which must also specify a slot. Likewise, if you configure a linkagg-peer without a slot, you must delete it before configuring a peer with a slot specified.

**Important**
Only one IPv4 or IPv6 BFD session-based configuration is allowed per link-agg interface for compliance with RFC 7130.

**Examples**
The following command configures linkage group 50 with IPv4 endpoints, a 50ms transmission interval, a 50ms interval for receiving control packets, and a compute hold-down time multiplier of 3.

```
bfd linkagg-peer 50 local-endpt-addr 2.2.2.1 remote-endpt-addr 2.2.2.2 interval 50 min_rx 50 multiplier 3
```
**bfd multihop-peer**

Configures parameters for any multihop-BFD sessions with the same destination address. If these parameters are not configured via this command, MH-BFD sessions with the same destination address will be in the Admin-down state.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BFD Configuration

configure > context context_name > bfd-protocol

Entering the above command sequence results in the following prompt:

`(context_name)host_name(config-bfd)#`

**Syntax Description**

```
bfd multihop-peer dst-ip-address { authentication { md5 | meticulous-md5 | meticulous-sha1 plain-text | sha1 } { encrypted password-string | password password-string } | interval tx Interval min_rx rx_interval multiplier value }
no bfd multihop-peer dst-ip-address authentication
```

**no**

Removes all the parameters for the MH-BFD destination address and if there are any sessions with the same destination address, those sessions will go to Admin-down state.

**dst-ip-address**

Specifies the destination address of the BFD enabled peer in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. This destination address must have been previously configured via the `ip route static bfd` or `ipv6 route static bfd` commands in the Context Configuration mode.

**authentication { md5 | meticulous-md5 | meticulous-sha1 plain-text | sha1 }**

Specifies the method for authenticating all multihop BFD sessions to the specified peer. By default, authentication for Multihop-BFD sessions to a destination address is disabled. The authentication type options include:

- **md5** – Message Digest 5
- **meticulous-md5** – MD5 using a secret key and sequence numbers updated for every packet
- **meticulous-sha1** – SHA1 with sequence numbers updated for every packet
• **plain-text** – plain text (unencrypted)

• **sha1** – Secured Hash Algorithm 1

**encrypted password-string | password password-string**

Specifies the password for authentication of BFD sessions. The password **must** be the same between the peer neighbors for the BFD sessions to work. If the authentication password is configured incorrectly between peers, the BFD sessions to the destination address will not come UP. If the password is configured for BFD sessions that are already UP, BFD neighbors will be reset.

• **encrypted password-string**: Specifies the use of an encrypted password for authentication of BFD sessions as an alphanumeric string of up to 523 characters.

• **password password-string**: Specifies the use of a plain text password for authentication of BFD sessions as an alphanumeric string of 1 through 19 characters.

**Important**

The destination address and its transmit/receive intervals must be configured **before** the password is applied to any MH-BFD sessions at a destination address.

**interval tx_interval min_rx rx_interval multiplier value**

**interval tx_interval**: Specifies the transmit interval (in milliseconds) between BFD packets as an integer from 50 through 999. Default: 50

**min_rx rx_interval**: Specifies the receive interval (in milliseconds) between BFD packets as an integer from 50 through 999. Default: 50

**multiplier value**: Specifies the multiplier value sued to compute holddown as an integer from 3 through 50. Default: 3

**Usage Guidelines**

Use this command to configure basic operating parameters between BFD enabled peers.

**Examples**

The following are example command strings for configuring BFD multihop sessions:

```
bfdf multihop-peer 10.2.3.4 authentication md5 encrypted 5-klm7783
bfdf multihop-peer 10.2.3.4 interval 100 min_rx 100 multiplier 5
```
**bfd nbr-group-name**

Configures BFD neighbor groups.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BFD Configuration

```
configure > context context_name > bfd-protocol
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-bfd)#
```

**Syntax Description**

| no | bfd nbr-group-name neighbor_group { active-if-name if_name | passive-if-name if_name } gw_ip_address
| no | bfd nbr-group-name neighbor_group

`no`

Removes all the parameters for the BFD neighbor group.

**neighbor_group**

Specifies an identifier for a BFD neighbor group as an alphanumeric string of 1 through 19 characters.

**active-if-name if_name | passive-if-name if_name**

Specifies the logical/physical interface associated with this BFD group.

**active-if-name if_name**: Specifies an active interface that notifies all passive interfaces in this group. There should be only one active interface in a group. `if_name` is a logical or physical interface specified as an alphanumeric string of 1 through 79 characters.

**passive-if-name if_name**: Specifies a passive interface that receives BFD notifications from the active interface in this group. `if_name` is a logical or physical interface specified as an alphanumeric string of 1 through 79 characters.

**gw_ip_address**

Specifies the gateway address of the BFD neighbor in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation (optional CIDR notation).
Usage Guidelines
Allow scaling of BFD sessions when a large number of logical interfaces are configured on a physical interface. A failure on the physical interface or a logical interface can be propagated to all passive interfaces in this group.

Examples
The following command configures BFD group bgpgrp132:
```
bfd nbr-group-name bgpgrp132 active-if-name bgpif02
```
**echo**

Enables or disables BFD echo mode functionality. The Echo function tests the forwarding path on the remote system. Echo is only used for single hop BFD sessions.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BFD Configuration

```configure > context context_name > bfd-protocol```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-bfd)#
```  

**Syntax Description**

| no | echo |

**no echo**

Disables BFD echo functionality.

**Usage Guidelines**

Use this function to send a stream of Echo packets that the other endpoint then sends back via its forwarding plane. Echo tests the forwarding path on the remote system.
**end**

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
`end`

**Usage Guidelines**
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 Description

d exit

Usage Guidelines

Use this command to return to the parent configuration mode.
slow-timers

Specifies the asynchronous mode control packet interval when Echo mode is enabled. In BFD asynchronous mode, BFD-enabled peers periodically send BFD Control packets to one another. If a number of those packets in a row are not received within the specified interval by the other peer, the session is declared to be down.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > BFD Configuration

```
configure > context context_name > bfd-protocol
```

Entering the above command sequence results in the following prompt:

```
{context_name} host_name(config-bfd) #
```

**Syntax Description**

```
slow-timers  timer_value
no slow-timers
```

*no*
Disables previously specified BFD slow timers.

*timer_value*
Specifies the BFD control packet interval (in milliseconds) for Echo mode as an integer from 1000 through 300000. Default: 2000

**Usage Guidelines**
Use this command to configure the interval between BFD control packets sent between peers in Echo mode.

**Examples**
The following example command configures an asynchronous mode control packet interval of 10000ms (10 seconds):
```
slow-timers 10000
```
slow-timers
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.

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

configure > context context_name > router bgp as_number > address-family address_family_type

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp-af-v6)#

---

**Important**

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

- end, page 1912
- exit, page 1913
- maximum-paths, page 1914
- neighbor, page 1916
- network, page 1920
- redistribute, page 1921
- timers bgp, page 1923


**end**

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

**Usage Guidelines**
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 Description**

exit

**Usage Guidelines**

Use this command to return to the parent configuration mode.
**maximum-paths**

Controls the maximum number of parallel external BGP (eBGP) or internal BGP (iBGP) routes that can be installed in a routing table.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

```plaintext
configure > context context_name > router bgp as_number > address-family address_family_type
```

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-bgp-af-v6)#
```

**Syntax Description**

```plaintext
[ no ] maximum-paths { ebgp num_paths | ibgp num_paths }
no maximum-paths { ebgp | ibgp }
```

no

Disables maximum paths for the specified route type command.

**maximum-paths ebgp num_paths**

Specifies the maximum number of parallel External Border Gateway Protocol routes as an integer from 1 through 10.

**maximum-paths ibgp num_paths**

Specifies the maximum number of parallel Internal Border Gateway Protocol routes as an integer from 1 through 10.

**Important**

If configured under the router-bgp-mode, multipath is enabled only for the prefixes learnt in the default-vrf. There is no support for vpnv4 prefixes even though multipath is turned on for the default-vrf.

If configured under the address-family-vrf-mode, multipath is enabled only for prefixes learnt in the vrf.
Usage Guidelines

Use this command to forward packets over multiple paths. User can control the maximum number of parallel eBGP routes that can be installed in a routing table. Enabling multipath does not affect the best path selection in BGP. If multipath is enabled, all the paths with the same weight, local-preference, as-path length, origin, and multi-exit discriminator (MED) as the best path are added to the routing table.

Examples

The following command disables forward of packets over multiple paths:

```
no maximum-paths ebgp
```
neighbor

Configures the IPv4/IPv6 Address Family for BGP routers that interconnect to non-broadcast networks.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

configure > context context_name > router bgp as_number > address-family address_family_type

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-bgp-af-v6)#

Syntax Description

| no | neighbor ip_address { activate | advertisement-interval adv_time | capability graceful-restart | default-originate | route-map map_name | distribute-list dist_list { in | out } | ebgp-multihop | max-hop number | encrypted password | encrypted_password | fall-over bfd multihop | filter-list filt_list { in | out } | max-prefix max_num | threshold thresh_percent | warning-only | next-hop-self | password | password | remote-as AS_num | remove-private-AS | restart-time rest_time | route-map map_name { in | out } | send-community { both | extended | standard } | shutdown | srp-activated-soft-clear | timers { connect-interval connect_interval | keepalive-interval keepalive_interval holdtime-interval holdtime_interval | min-peer-holdtime-interval min_peer_hold_interval | max-peer-holdtime-interval max_peer_hold_interval | connect-interval connect_interval | keepalive-interval keepalive_interval holdtime-interval holdtime_interval | connect-interval connect_interval | min-peer-holdtime-interval min_peer_hold_interval | update-source ip_address | weight value }

no
Delete the specified parameter from the router configuration.

neighbor ip_address

 Specifies the IP address of a BGP neighbor. ip_address must be in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

activate
Enables the exchange of routes with this neighbor.

advertisement-interval adv_time
Specifies the minimum interval (in seconds) between sending BGP routing updates.
adv_time must be an integer from 0 through 600. Default: 30

capability graceful-restart
Configures graceful re-start attributes.

default-originate [route-map map_name]
Specifies the default originate 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 }
Filters updates to and from this neighbor based on a route access list. Default: No filtering is performed.
dist_list is 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.

egp-multihop [max-hop number]
Allows eBGP neighbors that are not on directly connected networks.
max-hop number: Specifies the maximum number of hops allowed to reach a neighbor as an integer from 1 through 255. Default hop count: 255

encrypted password encryp_password
Specifies the encrypted password that is used only inside configuration files. This is an alphanumeric string of 1 through 24 characters.

fall-over bfd multihop
Supports Bidirectional Forwarding Detection (BFD) multihop for failover.

filter-list filt_list { in | out }
Establishes BGP filters based on an autonomous system (AS) path access list. filt_list is 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]
Specifies the maximum number of prefixes accepted from this peer. When the maximum is exceeded the neighbor connection is reset. max_num is an integer from 1 through 4294967295. Default: No maximum prefix limit.
threshold thresh_percent: Specifies a percentage value of when the BGP table is full. When this value is reached peer warnings are sent to the neighbor. thresh_percent must be an integer from 1 through 100.
warning-only: Specifies that only a warning message is sent when the limit is exceeded. The neighbor connection is not reset.
next-hop-self **ip_address**
Disables the next hop calculation for this neighbor.

**password password**
Sets a *password* expressed as an alphanumeric string of 1 through 24 characters.

**remote-as **AS_num**
Specify the AS number of the BGP neighbor as an integer from 1 through 4294967295.

**remove-private-AS**
Removes the private AS number from outbound updates. Default: Do not remove the private AS number.

**restart-time rest_time**
Specifies the maximum time (in seconds) required to for neighbor to restart as an integer from 1 through 3600.

**route-map **map_name** { in | out }**
Applies a route map to the neighbor. *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.

**send-community { both | extended | standard }**
Sends the community attributes to a peer router (neighbor).

**both**: Sends standard and extended community attributes

**extended**: Sends extended community attributes.

**standard**: Sends standard community attributes.

**shutdown**
Administratively shuts down this neighbor. This disables exchanging routes or configuring parameters for this neighbor.

**srp-activated-soft-clear**
Enables BGP updates when SRP-enabled resources are modified.

**timers **{ [ connect-interval connect_interval ] | [ keepalive-interval keepalive_interval holdtime-interval holdtime_interval ] }**
Sets BGP timers for the specified neighbor.

**connect-interval connect_interval**: Specifies the connect timer (in seconds) as an integer from 0 through 65535. The default is 60 seconds.

**keepalive-interval keepalive_interval**: Specifies 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** *holdtime_interval:* Specifies 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.

**min-peer-holdtime-interval** *min_peer_hold_interval:* Specifies the minimum acceptable hold time (in seconds) from peer for a keepalive message before declaring a neighbor dead. *min_peer_hold_interval* must be an integer from 0 through 65535. The default is 90 seconds.

**update-source** *ip_address*

Binds 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*

Sets the default weight for routes from this neighbor as an integer from 0 through 65535. Default: 0

### Usage Guidelines

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.

---

### Examples

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 (180 seconds):

```
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

Configures and specifies a network to announce via BGP.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

configure > context context_name > router bgp as_number > address-family address_family_type

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-bgp-af-v6)#

Syntax Description
| no | network ip_address/mask | route-map map_name |

no
Delete the specified network from the configuration for the BGP router.

network 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 IPV4 dotted-decimal notation and mask is the number of subnet bits, representing a subnet mask in CIDR. 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 as an alphanumeric string of 1 through 79 characters.

Usage Guidelines
Use this command to specify a network to announce via BGP.

Examples
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

Redistributes routes into BGP from another protocol as BGP neighbors.

Product: All

Privilege: Security Administrator, Administrator

Command Modes: Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

```
configure > context context_name > router bgp as_number > address-family address_family_type
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp-af-v6)#
```

Syntax Description:

```
[no] redistribute { connected | ospf | rip | static } [ route-map map_name ]
```

- **no**
  Remove the specified redistribution parameters from the BGP router configuration.

- **redistribute connected**
  Specifies that connected routes will be redistributed.

- **redistribute ospf**
  Specifies that Open Shortest Path First (OSPF) routes will be redistributed.

- **redistribute rip**
  Specifies that Routing Information Protocol (RIP) routes will be redistributed. (RIP is not supported at this time.)

- **redistribute static**
  Specifies that static routes will be redistributed.

- **route-map map_name**
  Filters routes through the specified route map before redistribution. map_name specifies the name of the route-map to use as an alphanumeric string of 1 through 79 characters.
Usage Guidelines

Use this command to specify what routes this BGP router should redistribute into BGP.

Examples

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
```
**timers bgp**

Enables or disables an aggressive minimum BGP route advertisement interval (MinRtAdvInterval) for ICSR configurations.

**Product**

All products that support ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

```
configure > context context_name > router bgp as_number > address-family address_family_type
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-bgp-af-v6)#
```

**Syntax Description**

```
[ no ] timers bgp icsr-aggr-advertisement-interval seconds
```

*no*

Disables this aggressive ICSR BGP advertisement interval.

*seconds*

Sets the number of seconds as an integer from 0 to 30. Default: 0.

**Usage Guidelines**

Use this command to configure an aggressive ICSR BGP advertisement interval (MinRtAdvInterval). The default value is 0. If set as 0, the aggressive advertisement interval is disabled.

The MinRtAdvInterval can be uniquely set for each address family.

After ICSR switchover, BGP will set the advertisement-interval for each AFI/SAFI (Address Family Identifier/Subsequent Address Family Identifier) supported by the peer to the configured value. BGP updates will be advertised to the peer based on this interval.

**Examples**

The following command sets the MinRtAdvInterval for this address family to 1 second:

```
timers bgp icsr-aggr-advertisement-interval 1
```
BGP Address-Family (VPNv4/VPNv6)
Configuration Mode Commands

The Border Gateway Protocol (BGP) Address-Family (VPNv4/VPNv6) Configuration Mode is used to configure the VPNv4 or VPNv6 address family information.

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

```
configure > context context_name > router bgp as_number > address-family address_family_type
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp-af-v4)#
```

**Important**

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

- end, page 1926
- exit, page 1927
- neighbor, page 1928
- timers bgp, page 1930
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

end

Usage Guidelines

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 Description**  
exit

**Usage Guidelines**  
Use this command to return to the parent configuration mode.
neighbor

Configures the VPNv4 or VPNv6 address family on BGP routers that interconnects to non-broadcast networks and enables the exchange of routing information with a peer router (neighbor).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

`configure > context context_name > router bgp as_number > address-family address_family_type`

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-bgp-af-v4)#
```

**Syntax Description**

```
[ no ] neighbor ip_address { activate | advertisement-interval interval_seconds | send-community { both | extended | standard } }
```

**no**

Delete the specified parameter from the router configuration.

**neighbor ip_address**

Specifies the IP address of the peer router (neighbor) in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**activate**

Enables the exchange of routing information with this neighbor.

**advertisement-interval interval_seconds**

Specifies the minimum interval in seconds between sending BGP routing updates as an integer from 0 through 600.

**send-community { both | extended | standard }**

Sends the community attributes to a peer router (neighbor).

- **both**: Sends standard and extended community attributes.
- **extended**: Sends extended community attributes.
**standard**: Sends standard community attributes.

**Usage Guidelines**

Use this command to enable the exchange of routing information with a peer router. The chassis supports a maximum of 64 peers per context.

**Examples**

The following command enables the exchange of routing information with the neighbor at IP address 192.168.100.25:

```
neighbor 192.168.100.25 activate
```
**timers bgp**

Enables or disables an aggressive minimum BGP route advertisement interval (MinRtAdvInterval) for ICSR configurations.

**Product**

All products that support ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

```
configure > context context_name > router bgp as_number > address-family address_family_type
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-bgp-af-v6)#
```

**Syntax Description**

```
[ no ] timers bgp icsr-aggr-advertisement-interval seconds
```

**no**

Disables this aggressive ICSR BGP advertisement interval.

**seconds**

Sets the number of seconds as an integer from 0 to 30. Default: 0.

**Usage Guidelines**

Use this command to configure an aggressive ICSR BGP advertisement interval (MinRtAdvInterval). The default value is 0. If set as 0, the aggressive advertisement interval is disabled.

The MinRtAdvInterval can be uniquely set for each address family.

After ICSR switchover, BGP will set the advertisement-interval for each AFI/SAFI (Address Family Identifier/Subsequent Address Family Identifier) supported by the peer to the configured value. BGP updates will be advertised to the peer based on this interval.

**Examples**

The following command sets the MinRtAdvInterval for this address family to 1 second:

```
timers bgp icsr-aggr-advertisement-interval 1
```
BGP Address-Family (VRF) Configuration Mode Commands

The Border Gateway Protocol (BGP) Address-Family (VRF) Configuration Mode is used to configure the Virtual Routing and Forwarding address family information.

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

configure > context context_name > router bgp as_number > address-family address_family_type

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp-af-vpnv4)#
```

**Important**

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

- end, page 1932
- exit, page 1933
- neighbor, page 1934
- redistribute, page 1938
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

dend

Usage Guidelines

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 Description**

exit

**Usage Guidelines**

Use this command to return to the parent configuration mode.
neighbor

Configures the Virtual Routing and Forwarding (VRF) address family for BGP routers that interconnect to non-broadcast networks.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

```
configure > context context_name > router bgp as_number > address-family address_family_type
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp-af-vpnv4)#
```

**Syntax Description**

```
[ 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 | srp-activated-soft-clear | 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.

**neighbor ip_address**

Specifies the IP address of the peer router (neighbor) in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**activate**

Enables 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 external BGP (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.

srp-activated-soft-clear
Enables BGP updates when SRP-enabled resources are modified.
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 Guidelines
Use this command to set parameters for communication with a specified neighbor. The chassis supports a
maximum of 64 peers per context.
A remote AS number must be specified for a neighbor before other parameters can be configured.

**Examples**

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 (180 seconds):

```
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
```
**redistribute**

Redistributes routes into BGP. This means that any routes from another protocol are redistributed to BGP neighbors using the BGP protocol.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

```
configure > context context_name > router bgp as_number > address-family address_family_type
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-bgp-af-vpnv4)#
```

**Syntax Description**

```
[ 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 Open Shortest Path First (OSPF) routes will be redistributed.

- **rip**
  Specifies that Routing Information Protocol (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 an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Use this command to specify what routes this BGP router should redistribute into BGP.

Examples

The following command redistributes OSPF routes after filtering them through the route map named Map1:

```bash
redistribute ospf route-map Map1
```

The following command removes the redistribution of OSPF routes from the router's configuration:

```bash
no redistribute ospf route-map Map1
```
redistribute
BGP Configuration Mode Commands

The Border Gateway Protocol (BGP) Configuration Mode is used to configure properties for BGP-4 routing.

Command Modes

Exec > Global Configuration > Context Configuration > BGP Configuration

configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp) #

Important

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

- accept-zero-as-rd, page 1943
- address-family ipv4, page 1944
- address-family ipv6, page 1946
- address-family vpv4, page 1947
- address-family vpv6, page 1948
- bgp, page 1949
- description, page 1950
- distance, page 1951
- end, page 1953
- enforce-first-as, page 1954
- exit, page 1955
- ip vrf, page 1956
- maximum-paths, page 1957
- neighbor, page 1958
- network, page 1963
- redistribute, page 1964
- router-id, page 1966
- scan-time, page 1967
- timers, page 1968
accept-zero-as-rd

Configures to accept VPN prefixes with Router Distinguisher (RD) value having Administrator Subfield, which is an Autonomous System number 0.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > BGP Configuration
configure > context context_name > router bgp as_number
Entering the above command sequence results in the following prompt:
<context_name>host_name(config-bgp)#

Syntax Description
[ no ] accept-zero-as-rd

no
Removes the configured VPN prefixes with RD value having AS number 0.

Usage Guidelines
Use this command to configure VPN prefixes with RD value having Administrator Subfield, which is an Autonomous System number 0.
By default the existing behavior of ASR5K will be preserved.

Examples
Following command configures to accept VPN prefixes with RD value having AS number 0:
accept-zero-as-rd
address-family ipv4

Enters the IPv4 Address Family configuration mode. Optionally, it also enables the Virtual Routing and Forwarding (VRF) routing configuration, if specified.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > BGP Configuration
configure > context context_name > router bgp as_number
Entering the above command sequence results in the following prompt:

\[(context_name)host_name(config-bgp)\#

**Syntax Description**
```plaintext
| no | address-family ipv4 | vrf vrf_name |
```

**Important**
The route distinguisher ID must be configured for the VRF name via the `route-distinguisher` command in BGP VRF Configuration mode, before using this keyword.

**vrf vrf_name**

Enables the exchange of VRF routing information. When this keyword is specified with this command, the address family mode changes to VRF address family mode. `vrf_name` is the name of an existing VFR expressed as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to configure the IPv4 BGP address family configuration parameters and optionally enables the exchange of VRF routing information.

Use of the `address-family ipv4` command switches the command mode to BGP Address Family Configuration Mode; the CLI prompt changes to:

\[(context_name)host_name(config-bgp-af-v4)\#\n

Use of `address-family ipv4 vrf vrf_name` command switches the command mode to BGP Address Family Configuration Mode; the CLI prompt changes to:

```
[context_name>\host_name(config-bgp-af-vrf)#
```

**Examples**

Use the 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**

Enters the IPv6 Address Family configuration mode. Optionally, it also enables the Virtual Routing and Forwarding (VRF) routing configuration mode, if specified.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration

```
configure > context context_name > router bgp as_number
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-bgp)#
```

**Syntax Description**

```
| no | address-family ipv6 | vrf vrf_name |
```

- **no**
  Removes the configured IPv6 address family VRF mode.

- **address-family ipv6**
  Enters the BGP Address-Family IPv6 mode to allow entry of IPv6 BGP parameters.

- **vrf vrf_name**
  Enables the exchange of VRF routing information. When this keyword is specified with this command, the address family mode changes to VRF address family mode. *vrf_name* is the name of an existing VFR expressed as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to configure the IPv6 BGP address family configuration parameters for BGP router.

Use of the **address-family ipv6** command switches the command mode to BGP Address Family Configuration Mode and changes the CLI prompt to:

```
<context_name>host_name(config-bgp-af-v6)#
```

**Examples**

Use the following command to enter the IPv6 BGP Address-Family configuration mode:

```
address-family ipv6
```
address-family vpnv4

Enters the IPv4 VPN Address Family configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > BGP Configuration

configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

\[context_name\]host_name(config-bgp)#

Syntax Description
address-family vpnv4

address-family vpnv4

Enters the BGP Address-Family IPv4 VPN mode to allow entry of VPN BGP parameters.

Usage Guidelines
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 the address-family vpnv4 command switches the command mode to BGP Address Family Configuration Mode; the CLI prompt changes to:

\[context_name\]host_name(config-bgp-af-vpnv4)#

Examples
Use the following command to enter the BGP Address-Family configuration mode for IPv4 VPN address parameters:

address-family vpnv4
address-family vpnv6

Enters the IPv6 VPN Address Family configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > BGP Configuration
configure > context context_name > router bgp as_number
Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-bgp)#

Syntax Description
address-family vpnv6

address-family vpnv6
Enters the BGP Address-Family IPv6 VPN mode to allow entry of VPN BGP parameters.

Usage Guidelines
Use this command to configure the IPv6 VPN 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 the address-family vpnv6 command switches the command mode to BGP Address Family Configuration Mode; the CLI prompt changes to:

{context_name}@host_name(config-bgp-af-vpnv6)#

Examples
Use the following command to enter the BGP Address-Family configuration mode for IPv6 VPN address parameters:
adress-family vpnv6
**bgp**

Defines the BGP-specific parameters regarding graceful restarts.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration

`configure > context context_name > router bgp as_number`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-bgp)#`

**Syntax Description**

`bgp graceful-restart { restart-time rest_time | stalepath-time stale_time | update-delay delay }`

`graceful-restart restart-time rest_time`

Specifies the maximum time (in seconds) required for neighbor(s) to gracefully restart. `rest_time` must be an integer from 1 through 3600.

`graceful-restart stalepath-time stale_time`

Specifies the maximum time (in seconds) to retain stale paths from restarting neighbor(s). `stale_time` must be an integer from 1 through 3600.

`graceful-restart update-delay delay`

Specifies the maximum time (in seconds) to defer initial route-selection. `delay` must be an integer from 1 through 3600.

**Usage Guidelines**

Use this command to set BGP-specific parameters regarding graceful restarts.

**Examples**

Use the following command to retain stale paths from restarting neighbor(s) for 100 seconds:

`bgp graceful-restart stalepath-time 100`
description

Allows you to enter descriptive text for this configuration.

Product All

Privilege Security Administrator, Administrator

Syntax Description
description text
no description

description text
Clears the description for this configuration.

text
Enter descriptive text as an alphanumeric string of 1 to 100 characters.
If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

Usage Guidelines
The description should provide useful information about this configuration.
distance

Defines the administrative distance for routes. The administrative distance is the default priority for a specific route or type route.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > BGP Configuration
configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp)#
```

**Syntax Description**
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 ] }

**no**
Removes the specified administrative distance for the specific route.

distance admin distance prefix prefix_addr | route-access-list list_name |

Sets the administrative distance to a specified value for routes with a specific IP prefix. If you also specify a route access list, the IP prefix must match the rules of that access list.

admin distance: Specifies the administrative distance that you want to apply to the IP prefix. *distance* must be an integer from 1 through 254.

prefix prefix_addr: Specifies the IP prefix of routes that should have the admin distance applied. *prefix_addr* must be an IPv4 address in dotted-decimal notation and the number of subnet bits, representing the subnet mask in CIDR shorthand (for example, 10.1.1.1/24).

route-access-list list_name: Defines the name of a route access list that defines for which routes the administrative distance should be set.

distance bgp external ebgp_dist internal ibgp_dist local local_dist

Sets the administrative distance for external (eBGP), internal (iBGP) and local routes.
**external ebgp_dist**: Sets the administrative distance for eBGP routes. `ebgp_dist` must be an integer from 1 through 254.

**internal ibgp_dist**: Sets the administrative distance for iBGP routes. `ibgp_dist` must be an integer from 1 through 254.

**local local_dist**: Sets the administrative distance for local routes. `local_dist` must be an integer from 1 through 254.

**Usage Guidelines**: 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.

**Examples**: 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 `rac11`:

```
distance admin 100 prefix 192.168.0.0/16 route-access-list rac11
```
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax Description
end

Usage Guidelines
Use this command to return to the Exec mode.
enforce-first-as

Enforces the first Autonomous System (AS) for Exterior Border Gateway Protocol (eBGP) routes. 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 (RFC 1930).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration

`configure > context context_name > router bgp as_number`

Entering the above command sequence results in the following prompt:

`{context_name}@host_name(config-bgp) #`

**Syntax Description**

`[ no ] enforce-first-as`

- no
  - Disables the enforcement of the first AS for Exterior Border Gateway Protocol (eBGP) routes.

- `enforce-first-as`
  - Enables the enforcement of the first AS for Exterior Border Gateway Protocol (eBGP) routes.

**Usage Guidelines**

Use this command to enforce the use of the first AS for EBGP routes.

**Examples**

Use the following command to enable this functionality:

`enforce-first-as`
exit

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

exit

Usage Guidelines

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

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**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration  
```bash
configure > context context_name > router bgp as_number
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp)#
```

**Syntax Description**

```
[ 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 an alphanumeric string of 1 through 79 characters identifying an existing instance.

**Usage Guidelines**

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; the CLI prompt changes to:

```
[context_name]>[host_name](config-bgp-vrf)#
```

**Examples**

The following command associates the pre-defined VRF context instance `router_mpls` to this BGP AS number:

```
ip vrf router_mpls
```
maximum-paths

Enables forwarding packets over multiple paths and specifies the maximum number of external BGP (eBGP) or internal BGP (iBGP) paths between neighbors.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > BGP Configuration

configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

`[context_name]host_name`(config-bgp) #

**Syntax Description**
maximum-paths { ebgp max_num | ibgp max_num }

[ no ] maximum-paths { ebgp | ibgp }

**no**
Disables forwarding packets over multiple eBGP or iBGP paths between neighbors.

**ebgp max_num**
Enables forwarding packets over multiple eBGP paths between neighbors and specifies the maximum number of eBGP paths. `max_num` must be an integer from 1 through 10 or 1 through 32 (VPC-DI only).

**ibgp max_num**
Enables forwarding packets over multiple iBGP paths between neighbors and specifies the maximum number of iBGP paths. `max_num` must be an integer from 1 through 10 or 1 through 32 (VPC-DI only).

**Usage Guidelines**
Use this command to enable or disable forwarding packets over multiple paths between neighbors and specify the maximum number of EBGP or IBGP paths.

**Examples**
To enable forwarding packets over multiple paths and set the maximum number of EBGP paths to 10, enter the following command:

```
maximum-paths ebgp 10
```

To disable forwarding packets over multiple EBGP paths, enter the following command:

```
no maximum-paths ebgp
```
**neighbor**

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**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration

configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-bgp)#
```

**Syntax Description**

```
no \[neighbor ip_address \{ activate | advertisement-interval adv_time | capability graceful-restart | default-originate \{ route-map map_name \} | distribute-list dist_list \{ in | out \} | ebgp-multihop \{ max-hop number \} | encrypted password encrypted-password | fall-over bfd \{ multihop \} | filter-list filt_list \{ in | out \} | max-prefix max_num | threshold thru_num | warning-only \} | next-hop-self | password password | remote-as AS_num | remove-private-AS | restart-time rest_time | route-map map_name \{ in | out \} | send-community \{ both | extended | standard \} | shutdown | srp-activated-soft-clear | 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.

**neighbor ip_address**

Specifies the IP address of a BGP neighbor. ip_address must be in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**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
The advertisement interval must be explicitly configured for an address family so that it can take effect for that address family. By default, it will be applicable only for the IPv4 address family. Specify the address family via the `address-family` command. You can then set the neighbor advertisement interval in the address family configuration mode.

**capability graceful-restart**
Configures BGP graceful restart attributes.

**default originate [ route-map map_name ]**
Enables the origination of 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 }**
Filters updates to and from this neighbor based on a route access list. `dist_list`: The name or number of an existing route-access-list. Default: No filtering is performed.

- `in`: Indicates that incoming advertised routes should be filtered.
- `out`: Indicates that outgoing advertised routes should be filtered.

**ebgp-multihop [ max-hop number ]**
Allows EBGP neighbors that are not on directly connected networks.

- `max-hop number`: Specifies the maximum number of hops allowed to reach a neighbor. `number` must be an integer from 1 through 255. Default hop count: 255

**encrypted password encrypted password**
Specifies an encrypted password that is used only inside configuration files. This should be an alphanumeric string of 1 through 523 characters.

**fall-over bfd [ multihop ]**
Enables Bidirectional Fwarping Detection (BFD) multihop support for failover.

This command adds or modifies a session in BFD for the BGP peer. If there is an existing session in BFD (same source-address/destination address), BGP or OSPF protocol will be added to the list of clients for the BFD session. BGP or OSPF will then be notified when there is a change in the BFD session state.

If there is no such BFD session, a new session is added in BFD. For MH-BFD, the session inherits the parameters including min-tx, min-rx, multiplier and authentication from the multihop-peer configuration in BFD by matching the destination address. If the parameters (interval) are not configured in BFD, then the BFD session will be in Admin-down state.

BGP adds a session in BFD only when the BGP peer is Established state. If there is a state transition in bgp where the peer is no longer in established state, then the bfd session is deleted. It will be added again, once the peer comes back to Established state.
filter-list \textit{filt_list} \{ in | out \}
Establishes BGP filters based on an AS path access list. \textit{filt_list} is the name of an existing AS path access list.
\textbf{in}: Indicates that incoming advertised routes will be filtered.
\textbf{out}: Indicates that outgoing advertised routes will be filtered.

\textbf{max-prefix} \textit{max_num} \{ threshold \textit{thresh_percent} \} \{ warning-only \}
The maximum number of prefixes accepted from this peer. When the maximum is exceeded the neighbor connection is reset.
Default: No maximum prefix limit.
\textit{max_num}: Specifies the maximum number of prefixes permitted. This must be an integer from 1 through 4294967295.
\{ threshold \textit{thresh_percent} \}: Specifies a percentage value of when the BGP table is full. When this value is reached, peer warnings are sent to the neighbor and the neighbor connection is reset. \textit{thresh_percent} must be an integer from 1 through 100.
\{ warning-only \}: Specifies that only a warning message is sent when the limit is exceeded. The neighbor connection is not reset.

\textbf{next-hop-self}
Disables the next hop calculation for this neighbor.

\textbf{password} \textit{password}
Specifies a password that is only used inside configuration files. This should be an alphanumeric string of 1 through 24 characters.

\textbf{remote-as} \textit{AS_num}
Specify the AS number of the BGP neighbor.
\textit{AS_num}: Specifies the neighbor's AS number as an integer from 1 through 65535.

\textbf{remove-private-AS}
Removes the private AS number from outbound updates. Default: Do not remove the private AS number.

\textbf{restart-time} \textit{rest_time}
Specifies the maximum time (in seconds) required for a neighbor to restart. \textit{rest_time} must be an integer between 1 and 3600.

\textbf{route-map} \textit{map_name} \{ in | out \}
Applies a route map to the neighbor. \textit{map_name} is the name of an existing route-map in the current context.
\textbf{in}: Indicates that the route map applies to incoming advertisements.
\textbf{out}: Indicates that the route map applies to outgoing advertisements.
send-community { both | extended | standard }
Sends the community attributes to a peer router (neighbor).

both: Sends extended and standard community attributes.
extended: Sends extended community attributes.
standard: Sends standard community attributes.

shutdown
Administratively shuts down this neighbor. This disables exchanging routes or configuring parameters for this neighbor.

srp-activated-soft-clear
Enables BGP updates when Service Redundancy Protocol SRP-enabled resources are modified.

timers { [ connect-interval conn_time ] | [ keepalive-interval keep_time holdtime-interval hold_time ] }
Specifies BGP timers for this 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
Binds 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
Sets the default weight for routes from this neighbor. value must be an integer from 0 through 65535. Default: 0

Usage Guidelines
Use this command to set parameters for communication with a specified neighbor. The chassis supports a maximum of 64 peers per context.

Examples
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 (180 seconds):

```
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**

Specifies a network to announce via BGP.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration

configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp) #

**Syntax Description**

[ 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 IPv4 address in dotted-decimal notation and mask is the number of subnet bits, representing a subnet mask in CIDR shorthand. These must be entered in the dotted-decimal notation/subnet bits format (for example, 10.1.1.1/24).

route-map map_name

Filter routes through the specified route map before announcing the network. map_name is the name of the route-map to use specified as an alphanumeric string of 1 through 79 characters.

**Usage Guidelines**

Use this command to specify a network to announce via BGP.

**Examples**

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

Redistributes routes via BGP from another protocol to BGP neighbors.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration

configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-bgp)#

**Syntax Description**

[ no ] redistribute { connected | ospf | rip | static } [ route-map map_name ]

**no**

Remove the specified redistribution parameters from the BGP router configuration.

**redistribute connected**

Specifies that connected routes will be redistributed.

**redistribute ospf**

Specifies that Open Shortest Path First (OSPF) routes will be redistributed

**redistribute rip**

Specifies that Routing Information Protocol (RIP) routes will be redistributed. (RIP is not supported at this time.)

**redistribute 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 an alphanumeric string of 1 through 79 characters.
Usage Guidelines

Use this command to specify what routes this BGP router should redistribute into BGP.

Examples

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

Overrides the configured router identifier and causes BGP peers to reset.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > BGP Configuration

configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

<context_name>host_name(config-bgp)#

Syntax Description

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.

router-id ip_address

Specifies the IP address to use as the BGP router ID as an IPv4 address in dotted-decimal notation.

Usage Guidelines

Use this command to configure a specific router ID that overrides the default.

Examples

The following command sets the router ID to 192.168.100.25:

router-id 192.168.100.25
**scan-time**

Configures the BGP background scanner interval. BGP monitors the next hop of the installed routes to verify next-hop reachability and to select, install, and validate the BGP best path. By default, the BGP scanner polls the Routing Information Base (RIB) for this information every 60 seconds. During the 60-second time period between scan cycles, Interior Gateway Protocol (IGP) instabilities or other network failures can cause temporarily black holes and routing loops.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BGP Configuration

configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp)#
```

**Syntax Description**

| no | scan-time time |

**no**

Remove the user specified scan time from the router's configuration. The scan time is reset to the default value.

**scan-time time**

Specifies 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. Default: 60

**Usage Guidelines**

Use this command to set the background scanner interval for the BGP router.

**Examples**

The following command sets the background scanner interval to 30 seconds:

```
scan-time 30
```
timers

Configures BGP routing timers.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > BGP Configuration
configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:
<context_name>host_name(config-bgp)#

Syntax Description
timers bgp keepalive-interval interval holdtime-interval time [ min-peer-holdtime-interval time ]

no
Remove the user specified timer values from the router's configuration. The timer values are reset to the default values.

Keepalive-interval interval: Specifies the interval (in seconds) to wait between sending keepalive packets as an integer from 0 through 65535. Default: 30

Holdtime-interval time: Specifies the interval (in seconds) after which the neighbor is considered dead if keepalive messages are not received as an integer from 0 through 65535.

[ min-peer-holdtime-interval time ]

Specifies the interval (in seconds) that is the minimum acceptable hold time from a neighbor as 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 Guidelines
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 a neighbor dead.
Examples

The following command sets the keepalive interval to 2 minutes (120 seconds) and the holdtime interval to 3 minutes (180 seconds):

```
timers bgp keepalive-interval 120 holdtime-interval 180 min-peer-holdtime-interval 0
```
BGP IP VRF Configuration Mode Commands

The Border Gateway Protocol (BGP) IP VRF (Virtual Routing and Forwarding) Configuration Mode is used to configure properties for BGP-4 routing.

**Important**

The VRF must have been preconfigured using the `ip vrf` command in the Context Configuration mode before you can enter this configuration mode.

**Command Modes**

```
Exec > Global Configuration > Context Configuration > BGP Configuration > BGP-IP VRF Configuration
configure > context context_name > router bgp as_number > ip vrf vrf_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp-vrf)#
```

**Important**

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

- end, page 1972
- exit, page 1973
- route-distinguisher, page 1974
- route-target, page 1976
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

end

Usage Guidelines

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 Description
exit

Usage Guidelines
Use this command to return to the parent configuration mode.
route-distinguisher

Assigns a route distinguisher (RD) for the VRF that helps identify a virtual routing domain in a provider's network and allows for overlapping IP space. The route distinguisher must be a unique value on the router for each VRF.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > BGP Configuration > BGP-IP VRF Configuration

configure > context context_name > router bgp as_number > ip vrf vrf_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-bgp-vrf)#

Syntax Description

route-distinguisher { as_number | ip_address } rd_identifier

route-distinguisher as_number rd_value

Identifies the target VRF by an autonomous system (AS) number. ASN value is a 16-bit ASN expressed as an integer from 0 through 65535.

route-distinguisher ip_address rd_value

Identifies the target VRF by its IP address. ip_address is entered using IPv4 dotted-decimal notation.

rd_identifier

rd_identifier is a unique route distinguisher identifier and must be an integer from 0 through 4294967295.

Usage Guidelines

Use this command to assign a router distinguisher (RD) for the IP VRF. The combination of AS number or 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 assigned to a VRF cannot be changed until the existing VRF is deleted or removed and reconfigured.
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 `10.5.3.4`:
```
route-distinguisher 10.5.3.4 12345
```
route-target

Adds an export and/or import list of extended route target communities to the VRF. BGP uses an extended-community attribute, the route target, to filter appropriate VPN routes into the correct VRFs. You configure the export list on the VRF to specify export route targets. When BGP advertises a route from this VRF's forwarding table, it associates the list of export route targets with the route and includes this attribute in the update message that advertises the route. You also configure a route-target import list on each VRF to specify import route targets.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > BGP Configuration > BGP-IP VRF Configuration
configure > context context_name > router bgp as_number > ip vrf vrf_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-bgp-vrf)#

Syntax Description
route-target { both | import | export } { as_value | ip_address } rt_value

route-target both
Creates a list of import and export route targets for the VRF with the same parameters. The list contains an AS number or IP address along with a route target (RT) value.

route-target import
Creates a list of import RTs for the VRF with the same parameters. The list contains an AS number or IP address along with an RT value.

route-target export
Creates a list of export RTs for the VRF with the same parameters. The list contains an AS number or IP address along with an RT value.

as_value
Specifies a 16-bit autonomous-system (AS) number expressed as an integer from 0 through 65535.
ip_address
Specifies an IP address in IPv4 dotted-decimal notation.

rt_value
Specifies a unique RT identifier as an integer from 0 through 4294967295.

Usage Guidelines
Use this command to create the list of export and/or import route target extended communities for VRF. A maximum of 5 route targets can be defined with this command up to release 9.0. A maximum 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 community.

Examples
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
BITS Port Configuration Mode Commands

The Building Integrated Timing Supply (BITS) port configuration mode allows you to configure an ASR 5000 SPIO equipped with an E1 or T1 BITS port. You can also configure line-timing whereby the SPIO recovers timing from a port on an optical (OLC/OLC2) or channelized (CLC/CLC2) card.

### Command Modes

Exec > Global Configuration > BITS Port Configuration

configure > port bits slot_number/port_number

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-port-slot_number/port_number)#
```

---

**Important**

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

- default, page 1980
- description, page 1981
- end, page 1982
- exit, page 1983
- mode, page 1984
- preferred slot, page 1985
- recover, page 1986
- shutdown, page 1988
- snmp trap link-status, page 1989
default

Restores the BITS port's default speed and communication mode.

Product  
SGSN

Privilege  
Security Administrator, Administrator

Command Modes  
Exec > Global Configuration > BITS Port Configuration

configure > port bits slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax Description

default { mode | preferred slot }

mode
Default: none
Sets the default for the ports framing mode.

preferred slot
Default: non-revertive
Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a port switch command to return service to the original port.

Usage Guidelines  
Restores port-level parameters to their default values.

Examples  
Use the following command to remove any setting for this port's framing mode:

default mode


**description**

Defines descriptive text that provides useful information about the BITS port.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > BITS Port Configuration

`configure > port bits slot_number/port_number`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-port-slot_number/port_number)#
```

**Syntax Description**

- **description** *text*
- **no**
- **description** *no description*

- **no**
  
  Removes 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 Guidelines**

Enter a description that provides helpful information, for example the BITS port's primary function, services, end users. Define any information, the only limit is the number of characters.

**Examples**

Use the following command to set a sample port description in the configuration file:

```
description samplePortDescriptiveText
```

Use the following command to set a more readable description:

```
description "This is a sample description"
```
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

dend

Usage Guidelines

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 Description**
exit

**Usage Guidelines**
Use this command to return to the parent configuration mode.
mode

Configures the framing mode for the port.

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > BITS Port Configuration

configure > port bits slot_number/port_number

Entering the above command sequence results in the following prompt:

[local] host_name (config-port-slot_number/port_number) #

Syntax Description
mode { e1 | t1 } framing type

e1 | t1

e1 selects the SDH E1 framing mode.
t1 selects the SONET T1 framing mode.

framing type

Specifies the type of framing used by E1 or T1 modes form which to derive timing:

- 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 Guidelines
Set the ports framing mode parameters.

Examples
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 SPIOs, one in slot 24 and the other in slot 25.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > BITS Port Configuration

```
configure > port bits slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax Description**

```
pREFERRED SLOT slot_number

[ default | no ] preferred slot slot_number
```

default

Defaults to non-revertive operation.

no

Disables revertive (auto-recovery) operation for the port.

**slot_number**

Identifies the physical slot in the chassis where the card is installed.

**Usage Guidelines**

This command enables or disables revertive port redundancy. So after a BITS 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 which requires an administrative user to manually issue a port switch command to return service to the original port.

**Examples**

Use this command to set the BITS port on the card in slot 25 as "preferred" for port redundancy:

```
pREFERRED Slot 25
```
recover

Configures line-timing so the SPIO recovers timing from a port on an optical (OLC/OLC2) or channelized (CLC/CLC2) card. The recovered clock is then distributed to synchronize timing on all line cards in the chassis.

---

**Important**

To employ line-timing recovery, the SPIO card(s) must be equipped with the optional Stratum 3 clock module.

---

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > BITS Port Configuration

`configure > port bits slot_number/port_number`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-port-slot_number/port_number)#
```

**Syntax Description**

```
recover { line1 slot_number | line2 slot_number }
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_number` is an integer between 1 and 48.

**line2 slot**

Sets second priority for line-timing clock recovered from the line card in the specified slot.

`slot_number` is an integer between 1 and 48. This cannot be the same slot number entered for **line1**.

**Usage Guidelines**

Define which line-timing source has priority.
Important

If the SPIO is connected to an external Building Integrated Timing Supply (BITS) source, BITS timing always takes precedence over line-timing.

Examples

Configure the line card in slot 19 as the preferred source for line-timing.

```
recover line 19
```
shutdown

Terminates all processes supporting the BITS 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

Command Modes

Exec > Global Configuration > BITS Port Configuration
configure > port bits slot_number/port_number

Entering the above command sequence results in the following prompt:

[local] host_name(config-port-slot_number/port_number)#

Syntax Description

| no | shutdown

no

Enables the port's administrative state. When omitted the card is shutdown (removed from service).

Usage Guidelines

Shut down a timing port prior to re-cabling and/or other maintenance activities.

This command with the no keyword is required to bring a port into service.

Examples

Use the following command to enable the port for service:

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

**Command Modes**
Exec > Global Configuration > BITS Port Configuration

configure > port bits slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

**Syntax Description**

| no | snmp trap link-status

**Usage Guidelines**

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.

**Examples**

Use this command to enable sending of link-status SNMP traps:

```shell
snmp trap link-status
```

Use this command to disable sending of link-status SNMP traps:

```shell
no snmp trap link-status
```
snmp trap link-status
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.

**Command Modes**

```
Exec > Global Configuration > Context Configuration > BMSC Profile Configuration
configure > context context_name > bmsc-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-bmsc-profile)#
```

**Important**

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

- `end`, page 1992
- `exit`, page 1993
- `gmb diameter dictionary`, page 1994
- `gmb diameter endpoint`, page 1995
- `gmb diameter peer-select`, page 1996
- `gmb user-data`, page 1998
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax Description
end

Usage Guidelines
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 Description

exit

Usage Guidelines

Use this command to return to the parent configuration mode.
gmb diameter dictionary

This command specifies the Diameter dictionary for the Gmb interface in the BMSC profile of an MBMS user service.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > BMSC Profile Configuration
configure > context context_name > bmsc-profile profile_name

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-bmsc-profile)#
```

**Syntax Description**
```
gmb 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 Guidelines**
Use this command to select the Gmb Diameter dictionary in BM-SC profile of MBMS user service.

**Examples**
The following command sets the Gmb Diameter dictionary to TS 29.061 (Rel. 7) specific:
```
gmb diameter dictionary standard
```
**gmb diameter endpoint**

This command specifies the Diameter endpoint name for the Gmb interface in the BMSC profile of an MBMS user service.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BMSC Profile Configuration

`configure > context context_name > bmsc-profile profile_name`

Entering the above command sequence results in the following prompt:

`{context_name}host_name(config-bmsc-profile)#`

**Syntax Description**

- `gmb diameter endpoint endpoint_name`
- `no gmb diameter endpoint`

`no`

Removes the previously configured Diameter endpoint name for the Gmb interface in the BMSC profile of an 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 alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to create a Gmb Diameter endpoint for a BMSC profile.

**Examples**

The following command creates a Diameter endpoint named `test1` in the BMSC profile of an MBMS user service:

`gmb diameter endpoint test1`
gmb diameter peer-select

This command specifies the peer ids of BM-C Diameter primary and secondary host in the BMSC profile for an MBMS user service.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > BMSC Profile Configuration
configure > context context_name > bmsc-profile profile_name

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-bmsc-profile)#
```

**Syntax Description**

gmb diameter peer-select peer peer_name | realm realm_name | secondary-peer sec_peer_name | realm sec_realm_name

**no**

Removes the previously configured BM-C Diameter peer ids configured in the BMSC profile of an MBMS user service.

**peer peer_name**

Specifyes the primary diameter host id for BMSC in this BMSC profile for MBMS user service. This is a unique name that is specified for the primary peer.

**realm realm_name**

Specifies the realm or domain for the Gmb Diameter peer. The realm may typically be a company or service name.

**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 fail-over processing.

**sec_peer_name** must be an alphanumeric string of 1 through 127 characters including punctuation marks.
realm sec_realm_name

Specifies the realm or domain for the Gmb Diameter secondary host. The realm may typically be a company or service name.

sec_realm_name must be an alphanumeric string of 1 through 127 characters including punctuation marks.

Usage Guidelines

Use this command to select a BMSC Diameter peer and realm in this BMSC profile for MBMS user service.

Examples

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 BMSC profile for user data for MBMS user service.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > BMSC Profile Configuration

```
configure > context context_name > bmsc-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-bmsc-profile)#
```

Syntax Description

```
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 the BMSC profile for user data of MBMS user service.

default

Sets the user data mode to unicast in the BMSC 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 BMSC to use as the outer destination address for the IP-in-IP tunnel to send multicast data, if the 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 Guidelines**

Use this command to configure user data mode and other parameters in the BMSC profile for user data of MBMS user service.

GGSN can receive multicast data from BMSC 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 the *mode-preference* keyword configures the GGSN's preferred mode for receiving multicast data.

**Important**

Both GGSN and BMSC must support the Unicast mode of multicast data transfer. If any GGSN or BMSC does not support Multicast mode, BMSC will transfer multicast data using Unicast mode only.

Use the *unicast-self-address* keyword to configure the GGSN's IP address which the BMSC 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.

**Examples**

The following command sets the MBMS data transfer mode to unicast:

default gmb user-data mode-preference

gmb user-data
BSSGP Cause Code Group Configuration Mode

Commands in this mode enable the operator to define multiple cause codes for the 2G service.

**Command Modes**

Exec > Global Configuration > LTE Policy Configuration > BSSGP Cause Code Configuration

configure > lte-policy > cause-code-group group_name protocol bssgp

Entering the above command sequence results in the following prompt:

[local] host_name (bssgp-cause-code)

---

**Important**

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

- end, page 2002
- exit, page 2003
- radio-cause, page 2004
**end**

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

end

**Usage Guidelines**

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 Description**
exit

**Usage Guidelines**
Use this command to return to the parent configuration mode.
radio-cause

Enables the operator to specify one or more cause codes for the 2G service.

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > LTE Policy Configuration > BSSGP Cause Code Configuration
configure > lte-policy > cause-code-group group_name protocol bssgp

Entering the above command sequence results in the following prompt:

[local] host_name (bssgp-cause-code)#

Syntax Description
radio-cause cause_code
no radio-cause cause_code

no
When included with the command, the specified cause code is deleted from the group. If all cause codes are deleted from the group then the group is automatically deleted.

cause_code
Enter an integer from 0 to 255 to identify a BSSGP protocol radio cause code, as defined in the Radio Cause section of the 3GPP TS 48.028 specification.

Important
The SGSN does not support Enhanced Radio Status functionality; therefore, the SGSN treats cause code values 0x03 and 0x04 as "Radio contact lost with MS". Therefore, the valid configurable cause codes values are 0, 1, and 2.

Usage Guidelines
The command can be repeated to define up to 16 BSSGP cause codes. This means that under each cause code group the maximum number of cause codes (ranap+bssgp+s1ap) that can be supported is 16.

Benefit of specifying the cause codes in a group:

- if the BSSGP radio cause code configured by the operator matches with the radio cause received in the Radio Status message, and
• if the Subscriber Overcharging Protection feature is enabled for 2G service in the GPRS-Service configuration,

• then the S4-SGSN includes ARRL (Abnormal Release of Radio Link) bit in Release Access Bearer Request message Initiated on Ready-to-Standby state transition.

Examples
 Repeat the command with different cause values to create a group:
 radio-cause 1
 radio-cause 3
radio-cause
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.

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.

Command Modes

Exec > Global Configuration > Bulk Statistics Configuration > Bulk-File Configuration
configure > bulkstats config_mode file file_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats-file-number)#

Important
The schema related commands in this configuration mode are identical to the same commands in the "Bulk Statistics Configuration Mode Commands" chapter.
The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
Bulk Statistics Configuration Mode Commands

Refer to the Common Syntax Options section in this chapter for information about formatting the output of bulk statistics.

---

**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.

---

The Bulk Statistics Configuration Mode is used to manage the options for the collection, formatting and delivery of system statistics to remote nodes.

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

```plaintext
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```plaintext
[local] host_name(config-bulkstats)#
```

---

**Important**

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

---

**Important**

In release 20.0 and higher Trusted StarOS builds, FTP is not supported. SFTP is the recommended file transfer protocol. For additional information, refer to the System Administration Guide.

---

- Overview, page 2013
- aal2 schema, page 2014
- alcap schema, page 2016
- apn schema, page 2018
- asngw schema, page 2020
• bcmcs schema, page 2022
• card schema, page 2024
• closedrp schema, page 2026
• context schema, page 2028
• cs-network-ranap schema, page 2030
• cs-network-rtp schema, page 2032
• cs-network-sccp schema, page 2034
• dcca schema, page 2036
• dcca-group schema, page 2038
• default, page 2040
• diameter-acct schema, page 2042
• diameter-auth schema, page 2044
• dlci-util schema, page 2046
• dpca schema, page 2048
• ecs schema, page 2050
• egtpc schema, page 2052
• end, page 2054
• exit, page 2055
• fa schema, page 2056
• file, page 2058
• fng schema, page 2060
• footer, page 2061
• gather-on-standby, page 2063
• gprs schema, page 2064
• gtpe schema, page 2066
• gtpp schema, page 2068
• gtpu schema, page 2070
• ha schema, page 2072
• header, page 2074
• hnbgw-hnbap schema, page 2076
• hnbgw-hnbap-access-closed schema, page 2078
• hnbgw-hnbap-access-hybrid schema, page 2080
• hnbgw-hnbap-access-open schema, page 2082
Bulk Statistics Configuration Mode Commands

- pcc-sp-endpt schema, page 2149
- pcc-service schema, page 2151
- pdif schema, page 2153
- pgw schema, page 2155
- port schema, page 2157
- ppp schema, page 2159
- ps-network-gtpu schema, page 2161
- ps-network-ranap schema, page 2163
- ps-network-sccp schema, page 2165
- radius schema, page 2167
- radius-group schema, page 2169
- receiver, page 2171
- remotefile, page 2173
- rlf schema, page 2175
- rlf-detailed schema, page 2177
- rp schema, page 2179
- saegw schema, page 2181
- sample-interval, page 2183
- sbc schema, page 2184
- sccp schema, page 2186
- schema, page 2188
- sgs schema, page 2190
- sgs-vlr schema, page 2192
- sgsn schema, page 2194
- sgtp schema, page 2196
- sgw schema, page 2198
- show variables, page 2200
- sls schema, page 2204
- ss7link schema, page 2206
- ss7rd schema, page 2208
- tai schema, page 2210
- transfer-interval, page 2212
- vlan-npu schema, page 2213
Overview

Schema Format String Syntax

The following defines common syntax block options. These options appear in similar commands and are detailed here for easy reference.

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. Supported Escape character shortcuts are "\n" for new line and "\t" for tab.

Enclosing an alphanumeric string within double quotation marks (" ") allows you to include spaces in the string.

Variables within the format string must be enclosed within "% and %", for example, "%var%". The actual variables supported are command-dependent and are described in the Statistics and Counters Reference (prior to Release 20.0) and in the Statistics and Counters spreadsheet (Release 20.0 and higher).

Schema Format String Length

The maximum length for a schema format specified via the CLI command cannot be more than 3599 characters long. The syntax is shown below.

```
<schema_type> schema <schema_name> format <schema_format>
```

Where:

- `<schema_name>` can be a maximum of 31 alphanumeric characters.
- `<schema_format>` can be a maximum of 3599 characters, including spaces within double quotation marks (" ").

Bulk Statistic Variables

For a list of the statistical variables (%var%) available for use in creating a schema format for each schema type:

- Run the Exec mode `show bulkstats variables schema_type` command.
- See the Statistics and Counters Overview chapter of the Statistics and Counters Reference (StarOS releases prior to 20.0) or the Statistics and Counters Reference spreadsheet (release 20.0 and higher).
**aal2 schema**

**Important**

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures the ATM adaptation layer 2 (AAL2) bulk statistics schema within an ATM virtual connection by the HNB-GW.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-bulkstats)#
```

**Syntax Description**

```
aal2 schema schema_name [active-only] format schema_format
no aal2 schema schema_name
```

**no**

Removes the specified schema.

```
schema_name
```

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**active-only**

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

```
format schema_format
```

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
For information on the schema format's syntax, see [Schema Format String Syntax, on page 2013.](#)

**Important**

For a complete list of the statistics that are supported for this schema, refer to the [Statistics and Counters Reference.](#)

---

**Usage Guidelines**

Use this command to define schemas for ATM adaptation layer 2 (AAL2) bulk statistics collection. Multiple AAL2 schemas can be created to further categorize HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple AAL2 schemas, re-issue the `aal2 schema schema_name` command using a different schema name.

You can also use this command to restrict the AAL2 schema statistics to those gathered on the Active ICSR chassis.

**Examples**

The following command creates a schema named `aal2stats1` that records the number of AAL2 uplink packets transmitted and AAL2 downlink packets received by Access Link Control Application Part (ALCAP) service on HNB-GW:

```
aal2 schema aal2stats1 format "%uplink-pkts-tx%" "%downlink-pkts-rx%"
```
alcap schema

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures the Access Link Control Application Part (ALCAP) bulk statistics schema for an ALCAP service on an HNB-GW node.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration
`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
alcap schema schema_name [active-only] format schema_format
no alcap schema schema_name
```

**no**
Removes the specified schema.

**schema_name**
Specifies the schema's name.
`schema_name` must be an alphanumeric string of 1 through 31 characters.

**active-only**
Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

**format schema_format**
Specifies the schema's format.
`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.

**Important**  
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage Guidelines**  
Use this command to define schemas for Access Link Control Application Part (ALCAP) service bulk statistics collection on HNB-GW node. Multiple ALCAP schemas can be created to further categorize at AAL2 channel-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple ALCAP schemas, re-issue the `alcap schema schema_name` command using a different schema name.

You can also use this command to restrict the ALCAP schema statistics to those gathered on the Active ICSR chassis.

**Examples**  
The following command creates a schema named `alcap1stats1` that records the number of AAL2 channels in connecting and connected state on ALCAP service:

```
alcap schema alcap1stats1 format "\%num-aal2-channels-in-connecting\%" "\%num-aal2-channels-in-connected-state\%"
```
**apn schema**

Configures the Access Point Name (APN) bulk statistics schema.

**Product**  
GGSN

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Bulk Statistics Configuration  
**configure > bulkstats mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
apn schema schema_name [active-only] format schema_format
no apn schema schema_name
```

- **no**
  
  Removes the specified schema.

- **schema_name**
  
  Specifies the schema's name.
  
  *schema_name* must be an alphanumeric string of 1 through 31 characters.

- **active-only**
  
  Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

- **format schema_format**
  
  Specifies the schema's format.
  
  *schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
  
  For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

---

**Important**

For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference.*
**Usage Guidelines**

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 schema_name` command using a different schema name.

You can also use this command to restrict the APN schema statistics to those gathered on the Active ICSR chassis.

**Examples**

The following command creates a schema named `apn1stats1` that records the number of sessions currently facilitated by the APN:

```
apn schema apn1stats1 format "%sess-curr%"
```
asngw schema

Configures Access Service Gateway (ASN-GW) bulk statistics schema.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:
[local]host_name(config-bulkstats)#

Syntax Description
asngw schema  schema_name  [active-only]  format  schema_format
no asngw schema  schema_name

no
Removes the specified schema.

schema_name
Specifies the schema's name.
schema_name must be an alphanumeric string of 1 through 31 characters.

active-only
Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

format  schema_format
Specifies the schema's format.
schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

Important
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

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 schema_name` command using a different schema name.

You can also use this command to restrict the ASN-GW schema statistics to those gathered on the Active ICSR chassis.

Examples

To create an ASN-GW schema named `asngw_statistics` that specifies a schema format of:

- VPN context name: `vpname`
- VPN Context Identifier: `vpid`
- 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: %vpname%
VPN ID: %vpid%
ASN-GW Service Name: %servname%
ASN-GW Service Identifier: %servid%
Peer IP Address: %peeripaddr%"
```
**bcmcs schema**

Configures Broadcast and Multicast Service (BCMCS) bulk statistics schema.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]\host_name(config-bulkstats)#

**Syntax Description**

```
bcmcs schema schema_name [active-only] format schema_format
no bcmcs schema schema_name
```

no

Removes the specified schema.

**schema_name**

Specifies the schema's name.

```
schema_name must be an alphanumeric string of 1 through 31 characters.
```

**active-only**

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

**format schema_format**

Specifies the schema's format.

```
schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
```

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

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 schema_name command using a different schema name.

You can also use this command to restrict the BCMCS schema statistics to those gathered on the Active ICSR chassis.

Examples

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

Configures card bulk statistics schema. These are statistics for circuit cards installed in the ASR 5x00 chassis.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax Description

\texttt{card \ scheme \ \textit{schema\_name} \ | \textit{active-only} | \textit{format} \ \textit{schema\_format} \no \ \texttt{card \ schema \ \textit{schema\_name}}}

\texttt{no}

Removes the specified schema.

\textit{schema\_name}

Specifies the schema's name.

\textit{schema\_name} must be an alphanumeric string of 1 through 31 characters.

\textit{active-only}

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

\textit{format \ \textit{schema\_format}}

Specifies the schema's format.

\textit{schema\_format} must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

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 schema_name` command using a different schema name.

You can also use this command to restrict the card schema statistics to those gathered on the Active ICSR chassis.

Important

Not supported on all platforms

Examples

The following command creates a schema named `card1stats1` that records the number of processes for all installed cards:

```
card schema card1stats1 format "%slot%-%numproc%
```

To create a card-level schema named `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%\nAvailable Memory: %memtotal%\nMemory Used (%): %memused%\nAvailable CPU (%): %cpuidle%"
```
closedrp schema

Configures Closed R-P bulk statistics schema.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax Description

closedrp schema  schema_name  [active-only]  format  schema_format

no closedrp schema  schema_name

no

Removes the specified schema.

schema_name

Specifies the schema's name.

schema_name must be an alphanumeric string of 1 through 31 characters.

active-only

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

format  schema_format

Specifies the schema's format.

schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

Important

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

This command defines schemas used for Closed R-P statistics collection. Multiple Closed R-P schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `closedrp schema schema_name` command using a different schema name.

You can also use this command to restrict the Closed R-P schema statistics to those gathered on the Active ICSR chassis.

Examples

The following command creates a schema named `closedrp1stats1` 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:

```
schema closedrp1stats1 format "%sess-curactive%-%sess-maxtunnel%"
```

To create a schema named `closedrpresourecostats` 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:

```
closedrp schema closedrpresourecostats format "Number of Successful Session Connections: %sess-successful%
Number of Session Attempts That Failed: %sess-failed%
Number of Sessions Currently Active: %sess-curative%"
```
**context schema**

Configures context bulk statistics schema.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax Description**

```
context schema schema_name [active-only] format schema_format
no context schema schema_name
```

**context schema**

Removes the specified schema.

**schema_name**

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**active-only**

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

**format schema_format**

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**

For the complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

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 schema_name` command using a different schema name.

You can also use this command to restrict the Context schema statistics to those gathered on the Active ICSR chassis.

Examples

To create a Firewall context schema named `sfw_context_stats1` that specifies a schema format of:

- Total packets received by firewall: `sfw-total-rxpackets`
- Total packets sent by firewall: `sfw-total-txpackets`
- Total ICMP packets discarded by firewall: `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%"
```
cs-network-ranap schema

Important

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.


Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local] host_name (config-bulkstats) #

Syntax Description

The syntax for the cs-network-ranap schema command is as follows:

cs-network-ranap schema schema_name [ active-only ] format schema_format

no cs-network-ranap schema schema_name

Syntax:

no

Removes the specified schema.

schema_name

Specifies the schema's name.

schema_name must be an alphanumeric string of 1 through 31 characters.

active-only

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

format schema_format

Specifies the schema's format.

schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage Guidelines**

Use this command to define schemas for RANAP procedure related bulk statistics collection in a CS network associated with HNB-GW in a Femto UMTS network. Multiple CS Networks RANAP schemas can be created to further categorize at CS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple CS Networks RANAP schemas, re-issue the `cs-network-ranap schema schema_name` command using a different schema name.

You can also use this command to restrict the RANAP schema statistics to those gathered on the Active ICSR chassis.

**Examples**

The following command creates a schema named `cs_ranap1stats1` that records the total number of Iu Release Request messages transmitted and total number of Iu Release Command message received by the HNB-GW node:

```plaintext
cs-network-ranap schema cs_ranap1stats1 format "%iu-rel-req-tx%" "%iu-rel-cmd-rx%"
```
cs-network-rtp schema

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures the Real-Time Transport Protocol (RTP) bulk statistics schema in a Circuit Switched (CS) network associated with an HNB-GW node.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:
[local]host_name(config-bulkstats)#

Syntax Description

- **cs-network-rtp schema** *schema_name* [**active-only**] [**format** *schema_format*

- **no**

  Removes the specified schema.

  *schema_name*

  Specifies the schema's name.

  *schema_name* must be an alphanumeric string of 1 through 31 characters.

- **active-only**

  Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

- **format** *schema_format*

  Specifies the schema's format.

  *schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.

**Important** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage Guidelines**

Use this command to define schemas for RTP procedure related bulk statistics collection in a CS network associated with HNB-GW in a Femto UMTS network. Multiple CS Networks RTP schemas can be created to further categorize at CS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple CS Networks RTP schemas, re-issue the `cs-network-rtp schema schema_name` command using a different schema name.

You can also use this command to restrict the RTP schema statistics to those gathered on the Active ICSR chassis.

**Examples**

The following command creates a schema named `cs_rtp1stats1` that records the total number of RTP Downlink Packets received and RTP Uplink Packets transmitted by HNB-GW node in an associated CS network:

```
cs-network-rtp schema cs_rtp1stats1 format "%rtp-uplink-pkts-tx%" "%rtp-downlink-pkts-rx%"
```
In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures the Signalling Connection Control Part (SCCP) bulk statistics schema in a Circuit Switched (CS) network associated with an HNB-GW node.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

- `cs-network-sccp schema schema_name [active-only] format schema_format`
- `no cs-network-sccp schema schema_name`

- **schema_name**
  - Specifies the schema's name.
  - `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **active-only**
  - Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

- **format schema_format**
  - Specifies the schema's format.
  - `schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

- **no**
  - Removes the specified schema.
Usage Guidelines

Use this command to define schemas for SCCP connection related bulk statistics collection in a CS network associated with HNB-GW in a Femto UMTS network. Multiple CS Networks SCCP schemas can be created to further categorize at CS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple CS Networks SCCP schemas, re-issue the `cs-network-sccp schema schema_name` command using a different schema name.

You can also use this command to restrict the SCCP schema statistics to those gathered on the Active ICSR chassis.

Examples

The following command creates a schema named `cs_sccp1stats1` that records the total number of SCCP connection requests received by HNB-GW and responses sent to CN node in an associated CS network:

```
cs-network-sccp schema cs_sccplstats1 format "%sccp-conn-req-rx%" "%sccp-conn-req-tx%"
```
**dcca schema**

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

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
dcca schema  schema_name  |  active-only  |  format  schema_format  
no  dcca schema  schema_name
```

- **no**
  - Removes the specified schema.

- **schema_name**
  - Specifies the schema's name.
  - *schema_name* must be an alphanumeric string of 1 through 31 characters.

- **active-only**
  - Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

- **format schema_format**
  - Specifies the schema's format.
  - *schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the **Schema Format String Length**, on page 2013 section.
  - For information on the schema format's syntax, see the **Schema Format String Syntax**, on page 2013 section.
Important  For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage Guidelines  Use this command to define schemas for DCCA bulk statistics collection.

You can also use this command to restrict the DCCA schema statistics to those gathered on the Active ICSR chassis.
**dcca-group schema**

This command configures Diameter Credit Control Application (DCCA) group bulk statistics schema. Please note that the DCCA-group related bulk statistics are copied from the "system" schema to this schema "dcca-group".

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
dcca-group schema  schema_name  [ active-only ]  format  schema_format
no dcca-group schema  schema_name

no
Removes the specified schema.

schema_name
Specifies the schema's name.

schema_name must be an alphanumeric string of 1 through 31 characters.

active-only
Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

format schema_format
Specifies the schema's format.

schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.
For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*

**Usage Guidelines**

Use this command to define schemas for DCCA group bulk statistics collection.

You can also use this command to restrict the DCCA group schema statistics to those gathered on the Active ICSR chassis.
default

Restores the system default for the option specified.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local] host_name(config-bulkstats)#

Syntax Description

default { limit | receiver mode | remotefile format | 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 Guidelines**

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.

**Examples**

- default limit
- default transfer-interval
diameter-acct schema

Configures Diameter Accounting bulk statistics schema. This command is available only in StarOS 11.0 and later releases.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

diameter-acct schema  *schema_name*  [active-only]  [format  *schema_format*]

no  diameter-acct schema  *schema_name*

no
Removes the specified schema.

*schema_name*

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

active-only

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

format  *schema_format*

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.
Important

For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage Guidelines

Use this command to define schemas for Diameter Accounting bulk statistics collection.

You can also use this command to restrict the Diameter Accounting schema statistics to those gathered on the Active ICSR chassis.
diameter-auth schema

Configures Diameter Authentication bulk statistics schema. This command is available only in StarOS 11.0 and later releases.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-bulkstats) #
```

**Syntax Description**

```
diameter-auth schema  schema_name  [active-only] [format  schema_format]
no  diameter-auth schema  schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema's name.
  *schema_name* must be an alphanumeric string of 1 through 31 characters.

- **active-only**
  Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

- **format schema_format**
  Specifies the schema's format.
  *schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
  For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.
For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage Guidelines**

Use this command to define schemas for Diameter Authentication bulk statistics collection.

You can also use this command to restrict the Diameter Authentication schema statistics to those gathered on the Active ICSR chassis.
dlci-util schema

Configures the collection of statistics for the DLCI-Util (DLCI utilization) schema.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration  
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
dlci-util schema  schema_name  [ active-only ]  format  schema_format  
no dlci-util schema  schema_name
```

**no**

Removes the specified schema.

**schema_name**

Specifies the schema's name.  
*schema_name* must be an alphanumeric string of 1 through 31 characters.

**active-only**

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

**format schema_format**

Specifies the format of the collected DLCI utilization statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.
Important

For a complete list of the statistics that are supported for the DLCI-Util schema, refer to the Statistics and Counters Reference.

Usage Guidelines

Use this command to define schemas for DLCI-Util bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple schemas can be created to categorize DLCI-Util bulk statistics. All of the schemas are processed at each collection interval. To create multiple DLCI-Util schemas, re-issue the `dlci-util schema schema_name` command using a different schema name each time.

You can also use this command to restrict the DLCI-Util schema statistics to those gathered on the Active ICSR chassis.

Examples

Include the bulk statistic variable names to create a schema named `dlciutilstats_sgsn1` that specifies collection of statistics (a schema format) for:

- card
- port
- path
- DS1/E1
- DLCI
- DLCI utilization snapshot for received packets
- DLCI utilization for received packets in the last 5 minutes
- DLCI utilization for received packets in the last 15 minutes

Use the following command:

```
gprs schema gprsstats_sgsn1 format "Card: %card%
Port: %port%
DLCI in path: %dlci_util_path%
DSI/E1: %dlci_util_ds1e1%
DLCI ID: %dlci_util_dlc_i
Current Rx: %dlci_util_dlc_i_curr_rx%
Rx in 5 minutes: %dlci_util_dlc_i_5min_rx%
Rx in 15 minutes: %dlci_util_dlc_i_15min_rx%"```
dpca schema

Configures Diameter Policy Control Application (DPCA) bulk statistics schema.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:
[local]host_name(config-bulkstats)#

Syntax Description

dpca schema  schema_name  | active-only  | format  schema_format
no dpca schema  schema_name

no
Removes the specified schema.

schema_name
Specifies the schema's name.
schema_name must be an alphanumeric string of 1 through 31 characters.

active-only
Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

format  schema_format
Specifies the schema's format.
schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

Important
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
**Usage Guidelines**

Use this command to define schemas for DPCA bulk statistics collection.

You can also use this command to restrict the DPCA schema statistics to those gathered on the Active ICSR chassis.
**ecs schema**

Configures Enhanced Charging Service (ECS) bulk statistics schema.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-bulkstats)#
```

**Syntax Description**

```
ecs schema schema_name [active-only] format schema_format
no ecs schema schema_name
```

**no**

Removes the specified schema.

`schema_name`

Specifies the schema's name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

**active-only**

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

`format schema_format`

Specifies the schema's format.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (`" "). For more information, see the **Schema Format String Length** on page 2013 section.

For information on the schema format's syntax, see the **Schema Format String Syntax**, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the **Statistics and Counters Reference**.
**Usage Guidelines**

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 schema_name` command using a different schema name.

You can also use this command to restrict the ECS schema statistics to those gathered on the Active ICSR chassis.
egtpc schema

Configures the enhanced GTP-C statistics schema for naming conventions of data files.

**Product**

- MME
- P-GW
- S-GW
- SAEGW
- SGSN

**Privilege**

Administrator

**Command Modes**

- Exec > Global Configuration > Bulk Statistics Configuration
- configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```plaintext
egtpc schema schema_name [ active-only ] format schema_format

no egtpc schema schema_name
```

- **no**
  - Removes the specified schema.

- **schema_name**
  - Specifies the schema’s name.
  - `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **active-only**
  - Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

- **format schema_format**
  - Specifies the schema’s format.
  - `schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

### Usage Guidelines

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 schema_name` command using a different schema name.

You can also use this command to restrict the GTP-C schema statistics to those gathered on the Active ICSR chassis.

### Examples

For an eGTP-C-level schema named `egtpcservicestats` that specifies a schema format of:

- Tunnel - Create Session Request Sent: `tun-sent-cresess`
- Tunnel - Create Session Request Received: `tun-recv-cresess`

Use the following command:

```
egtpc schema egtpcservicestats format "Number of GTP Tunnel Requests Sent: \%tun-sent-cresess\n\%tun-rev-cresess\n\nNumber of GTP Tunnel Requests Received: \%tun-recv-cresess\n"
```
### end

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

<table>
<thead>
<tr>
<th><strong>Product</strong></th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privilege</strong></td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

| **Syntax Description** | end |

| **Usage Guidelines** | 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 Description**

`exit`

**Usage Guidelines**

Use this command to return to the parent configuration mode.
fa schema

Configures Foreign Agent (FA) bulk statistics schema.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax Description**

fa schema  
no fa schema

```
schema_name  
active-only  
format   
```

**no**
Removes the specified schema.

```
schema_name  
```

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

```
active-only  
```

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

```
format  
```

Specifies the schema's format.

*format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the *Schema Format String Length*, on page 2013 section.

For information on the schema format's syntax, see the *Schema Format String Syntax*, on page 2013 section.

---

**Important**
For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*. 

---
Usage Guidelines

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 schema_name` command using a different schema name.

You can also use this command to restrict the FA schema statistics to those gathered on the Active ICSR chassis.

Examples

To create a FA-level schema named `faservicestats` that separates the `date`, `time`, and `vpname` by tabs, enter the following command:

```
fa schema faservicestats format %date%\t%time%\t%vpname%
```

The schema format appears as follows:

```
date  time  vpname
```
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

Command Modes
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax Description

| no | file number |

no
Removes a previously configured bulk statistic file.

number
Specifies a number for the bulkstatistics file as an integer from 1 through 4. This number is how the file is recognized by the system.

Usage Guidelines

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 four 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, 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.
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.

**Examples**

The following command creates a bulk statistics file numbered 2 and enters the Bulk Statistics File Configuration Mode:

```
file 2
```
fng schema

Configures Femto Network Gateway (FNG) bulk statistics schema.

**Product**

FNG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local] host_name (config-bulkstats)#

**Syntax Description**

```
fng schema schema_name format schema_format
no fng schema schema_name
```

**no**

Removes the specified schema.

**schema_name**

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**format schema_format**

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the *Schema Format String Length*, on page 2013 section.

For information on the schema format's syntax, see the *Schema Format String Syntax*, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*. 
**footer**

Configures the footer string placed at the end of the generated bulk statistics data files.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

**configure > bulkstats mode**

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-bulkstats) #
```

**Syntax Description**

- **footer format** `schema_format`
- **no footer format**

**no**

Clears the footer format string which results in the default file footer being used in generated data files.

- **format schema_format**

  Specifies the footer format string for use in generated data files.

  `schema_format` must be an alphanumeric string from 1 through 2047 characters. The format string syntax is described in the [Schema Format String Syntax, on page 2013](#) section. Default: "" (an empty footer)

The following variables are supported:

**Table 21: footer Command Format String Variables**

<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>
</tbody>
</table>
### Variable Description Data Type

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<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 Guidelines

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.

### Examples

The following commands define different footer formats:
- `footer format northStreet`
- `footer format "Created on: %date%-%time% by %host%"
- `no footer format`
**gather-on-standby**

Controls whether or not statistics are gathered when a system is in the standby state.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax Description**

<table>
<thead>
<tr>
<th>no</th>
<th>default</th>
<th>gather-on-standby</th>
</tr>
</thead>
</table>

**no**

Does not gather bulk statistics when the system is in the standby state.

**default**

Resets this command to its default action of gathering bulk statistics when the system is in the standby state.

**Usage Guidelines**

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 systems configured for Interchassis Session Recovery (ICSR). 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. However, no additional statistics gathering takes place.

**Examples**

The following command disables gathering statistics when the system is in the standby state:

```plaintext
no gather-on-standby
```

The following command enables the gathering of statistics when the system is in the standby state:

```plaintext
gather-on-standby
```
**gprs schema**

Configures the collection of statistics for the GPRS schema.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local] host_name(config-bulkstats)#

**Syntax Description**

`gprs schema schema_name [ active-only ] format schema_format`

`no gprs schema schema_name`

**no**

Removes the specified schema.

`schema_name`

Specifies the schema's name.

`schema_name` must be an alphanumeric string of 1 to 31 characters.

`active-only`

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

`format schema_format`

Specifies the format of the collected GPRS statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.
For a complete list of the statistics that are supported for the GPRS schema, refer to the Statistics and Counters Reference.

Important

Usage Guidelines

Use this command to define schemas for GPRS bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple GPRS schemas can be created to categorize GPRS bulk statistics. All of the schemas are processed at each collection interval. To create multiple GPRS schemas, re-issue the gprs schema schema_name command using a different schema name each time.

You can also use this command to restrict the GPRS schema statistics to those gathered on the Active ICSR chassis.

Examples

Include the bulk statistic variable names to create a GPRS schema named gprsstats_sgsn1 that specifies collection of statistics (a schema format) for:

- context name
- GPRS service name
- number of LLC packets dropped

Use the following command:

```
gprs schema gprsstats_sgsn1 format "Context Name: %vpname%\nGPRS Service Name: %servname%\nTotal LLC Packets Dropped: %bssgp-total-usr-req-drop%\n"
```
gtpc schema

Configures GPRS Tunneling Protocol-Control (GTPC) message statistics schema.

**Product**
- GGSN
- P-GW
- S-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Bulk Statistics Configuration
- configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
gtpc schema  | active-only | format  schema_format
no gtpc schema
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema's name.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **active-only**
  Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

- **format schema_format**
  Specifies the schema's format.
  `schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
  For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.
Usage Guidelines

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 schema_name` command using a different schema name.

You can also use this command to restrict the GTPC schema statistics to those gathered on the Active ICSR chassis.

Examples

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

Configures GPRS Tunneling Protocol-Prime (GTPP) statistics schema.

**Product**
- GGSN
- SGSN
- P-GW
- S-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
gtpp schema schema_name | active-only | format schema_format
no gtpp schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema's name.
  *schema_name* must be an alphanumeric string of 1 through 31 characters.

- **active-only**
  Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

- **format schema_format**
  Specifies the schema's format.
  *schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

Important

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage Guidelines

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 schema_name` command using a different schema name.

You can also use this command to restrict the GTPP schema statistics to those gathered on the Active ICSR chassis.

Examples

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"
```
**gtpu schema**

Configures GTP-U bulk statistics schema.

**Important**

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

**Product**

GGSN  
HNB-GW  
P-GW  
S-GW  
SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration  
**configure > bulkstats mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
gtpu schema schema_name [ active-only ] [ format schema_format ]  
no gtpu schema schema_name
```

- **no**  
  Removes the specified schema.
  
- **schema_name**  
  Specifies the schema's name.  
  **schema_name** must be an alphanumeric string of 1 through 31 characters.

- **active-only**  
  Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.
format schema_format

Specifies the format of the collected GTP-U statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages.

schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.

Important  For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage Guidelines

Use this command to define schemas for GTP-U bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple GTP-U schemas can be created to categorize GTP-U bulk statistics. All of the schemas are processed at each collection interval. To create multiple GTP-U schemas, re-issue the gtpu schema schema_name command using a different schema name each time.

You can also use this command to restrict the GTP-U schema statistics to those gathered on the Active ICSR chassis.
**ha schema**

Configures Home Agent (HA) bulk statistics schema.

**Product** HA

**Privilege** Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Bulk Statistics Configuration
- configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
ha schema | active-only | format
no ha schema
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema's name.
  *.schema_name* must be an alphanumeric string of 1 through 31 characters.

- **active-only**
  Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

- **format schema_format**
  Specifies the schema's format.
  *schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
  For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
**Usage Guidelines**

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 schema_name` command using a different schema name.

You can also use this command to restrict the HA schema statistics to those gathered on the Active ICSR chassis.

**Examples**

For an HA schema named `haservicestats` that specifies a schema format of:

- Number of HA authentication failures: `reply-haauthfail`
- Number of Mobile Node authentication failures: `reply-mnauthfail`

Use the following command:

```
ha schema haservicestats format "Number of HA authentication failures: %reply-haauthfail%\nNumber of Mobile Node authentication failures: %reply-mnauthfail%\n"
```
header

Configures the header string placed at the beginning of the generated bulk statistics data files.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

```bash
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-bulkstats) #
```

**Syntax Description**

- **header format schema_format**
- **no header format**

- **no**
  
  Clears the header format string which results in the default file header being used in generated data files.

- **format schema_format**
  
  Specifies the header format string for use in generated data files.

  *schema_format* must be an alphanumeric string of 1 through 2047 characters. The format string syntax is described in the Schema Format String Syntax, on page 2013 section. Default: "" (an empty header)

The following variables are supported:

**Table 22: header Command Format String Variables**

<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>Variable</td>
<td>Description</td>
<td>Data Type</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>-----------</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 Guidelines**

Define a unique header in data files which allows for easy identification as to which system generated the data file or any other useful information.

Using the variables described above allows 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.

**Examples**

The following commands define different header formats:

```plaintext
header format northStreet
header format "Created on: %date%-%time% by %host%"
no header format
```
In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures bulk statistics schema for HNB-Application Part (HNB-AP) message statistics collection in HNB-GW session instance.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

class > bulkstats mode

Entering the above command sequence results in the following prompt:

[local] host_name(config-bulkstats)#

**Syntax Description**

- **hnbgw-hnbap schema schema_name format schema_format**

  - **no** hnbgw-hnbap schema schema_name

  - **no**

    Removes the configured HNB-GW-HNB-AP schema.

  - **schema_name**

    Specifies a name for the HNB-GW-HNB-AP schema.

    **schema_name** must be an alphanumeric string of 1 through 31 characters.

  - **format schema_format**

    Specifies the schema's format.

    **schema_format** must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

    For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.
Usage Guidelines

This command defines schemas used for HNB-AP statistics collection. Multiple HNB-AP schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-hnbap schema schema_name` command using a different schema name.

Examples

The following command creates a schema named `hnbap1stats1` that records the number of registered UEs and registered HNBs along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-hnbap schema hnbap1stats1 format "\%vpnname\%-%vpnid\%-%servname\%-%registered-hnb\%-%registered-ue\%"
```

To create a schema named `hnbapuestats` that specifies a schema format of:

- Number of UEs with CS and PS Core Network Connections: `ue-with-ps-cs-conn`
- Number of UEs in Idle Condition: `idle-ue`

Use the following command:

```
hnbgw-hnbap schema hnbapuestats format "\Number of UEs with CS and PS Core Network Connections: \ue-with-ps-cs-conn\Number of UEs in Idle Condition: \idle-ue\"
```
In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures bulk statistics schema for HNB-Application Part (HNB-AP) message statistics collection in HNB-GW session instance for closed access mode.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
hnbgw-hnbap-access-closed schema  
schema_name format  
schema_format  

no hnbgw-hnbap-access-closed schema  
schema_name

no

Removes the configured HNB-GW-HNB-AP-ACCESS-CLOSED schema.

**schema_name**

Specifies a name for the HNB-GW-HNB-AP-ACCESS-CLOSED schema. **schema_name** must be an alphanumeric string of 1 through 31 characters.

**format schema_format**

Specifies the schema's format. **schema_format** must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the **Schema Format String Length**, on page 2013 section.

For information on the schema format's syntax, see **Schema Format String Syntax**, on page 2013.
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage Guidelines**

This command defines schemas used for HNB-AP statistics collection in closed access mode. Multiple HNB-AP-ACCESS-CLOSED schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-hnbap-access-closed schema schema_name` command using a different schema name.

**Examples**

The following command creates a schema named `hnbapclosed1stats1` that records the number of registered UEs and registered HNBs along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-hnbap-access-closed schema hnbapclosed1stats1 format "\%vpnname\%-%vpnid\%-%servname\%-%registered-hnb\%-%registered-ue\%"
```

To create a schema named `hnbapaccesscloseduestats` that specifies a schema format of:

- Number of UEs with CS and PS Core Network Connections: `ue-with-ps-cs-conn`
- Number of UEs in Idle Condition: `idle-ue`

Use the following command:

```
hnbgw-hnbap-access-closed schema hnbapaccesscloseduestats format "Number of UEs with CS and PS Core Network Connections: %ue-with-ps-cs-conn%\nNumber of UEs in Idle Condition: %idle-ue%"
```
**hnbgw-hnbap-access-hybrid schema**

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.</td>
</tr>
</tbody>
</table>

Configures bulk statistics schema for HNB-Application Part (HNB-AP) message statistics collection in HNB-GW session instance for hybrid access mode.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
hnbgw-hnbap-access-hybrid schema schema_name format schema_format
no hnbgw-hnbap-access-hybrid schema schema_name
```

- **no**
  Removes the configured HNB-GW-HNB-AP-ACCESS-HYBRID schema.

- **schema_name**
  Specifies a name for the HNB-GW-HNB-AP-ACCESS-HYBRID schema.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the schema's format.

  `schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

  For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.
For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage Guidelines**

This command defines schemas used for HNB-AP statistics collection in hybrid access mode. Multiple HNB-AP-ACCESS-HYBRID schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-hnbap-access-hybrid schema schema_name` command using a different schema name.

**Examples**

The following command creates a schema named `hnbaphyb1stats1` that records the number of registered UEs and registered HNBs along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-hnbap-access-hybrid schema hnbaphyb1stats1 format "\%vpnname\%-%vpnid\%-%servname\%-%registered-hnb\%-%registered-ue\%"
```

To create a schema named `hnbapaccesshybuestats` that specifies a schema format of:

- Number of UEs with CS and PS Core Network Connections: `ue-with-ps-cs-conn`
- Number of UEs in Idle Condition: `idle-ue`

Use the following command:

```
hnbgw-hnbap-access-hybrid schema hnbapaccesshybuestats format "Number of UEs with CS and PS Core Network Connections: %ue-with-ps-cs-conn%\nNumber of UEs in Idle Condition: %idle-ue%"
```
hnbgw-hnbap-access-open schema

**Important**
In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures bulk statistics schema for HNB-Application Part (HNB-AP) message statistics collection in HNB-GW session instance for open access mode.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
hnbgw-hnbap-access-open schema schema_name format schema_format
no hnbgw-hnbap-access-open schema schema_name
```

**no**
Removes the configured HNB-AP-ACCESS-OPEN schema.

**schema_name**
Specifies a name for the HNB-AP-ACCESS-OPEN schema.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**format schema_format**
Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the *Schema Format String Length*, on page 2013 section.

For information on the schema format's syntax, see *Schema Format String Syntax*, on page 2013.
Important

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage Guidelines

This command defines schemas used for HNB-AP statistics collection in open access mode. Multiple HNB-AP-ACCESS-OPEN schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-hnbap-access-open schema schema_name` command using a different schema name.

Examples

The following command creates a schema named `hnbapopen1stats1` that records the number of registered UEs and registered HNBs along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-hnbap-access-open schema hnbapopen1stats1 format
"%vpnname%-%vpnid%-%servname%-%registered-hnb%-%registered-ue%"
```

To create a schema named `hnbapacccessopenuestats` that specifies a schema format of:

- Number of UEs with CS and PS Core Network Connections: `ue-with-ps-cs-conn`
- Number of UEs in Idle Condition: `idle-ue`

Use the following command:

```
hnbgw-hnbap-access-open schema hnbapacccessopenuestats format "Number of UEs with CS and PS Core Network Connections: %ue-with-ps-cs-conn\nNumber of UEs in Idle Condition: %idle-ue%"
```
**hnbgw-ranap schema**

**Important**

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.


**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
hnbgw-ranap schema  schema_name  format  schema_format
no hnbgw-ranap schema  schema_name
```

- **no**
  - Removes the configured HNB-GW-RANAP schema.

- **schema_name**
  - Specifies a name for the HNB-GW-RANAP schema.
  - `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  - Specifies the schema's format.
  - `schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
  - For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Important**

This command defines schemas used for RANAP messaging statistics collection. Multiple RANAP schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-ranap schema schema_name` command using a different schema name.

**Usage Guidelines**

The following command creates a schema named `ranap1stats1` that records the number of CS-Direct-Transfer messages sent and received on RANAP along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-ranap schema ranap1stats1 format
"%vpnname%-%vpnid%-%servname%-%cs-dir-transfer-rx%-%cs-dir-transfer-tx%"
```

To create a schema named `ranappagingstats` that specifies a schema format of:

- Number of paging requests sent on RANAP from CS Core Network Connections: `cs-paging-req-tx`
- Number of paging requests sent on RANAP from PS Core Network Connections: `ps-paging-req-tx`

Use the following command:

```
hnbgw-ranap schema ranappagingstats format "Number of paging requests sent on RANAP from CS Core Network Connections: %cs-paging-req-tx%
Number of paging requests sent on RANAP from PS Core Network Connections: %ps-paging-req-tx%"
```
In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.


**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
hnbgw-ranap-access-closedschema schema_name format schema_format
no hnbgw-ranap-access-closedschema schema_name
```

- **no**
  
  Removes the configured HNB-GW-RANAP-ACCESS-CLOSED schema.

- **schema_name**
  
  Specifies a name for the HNB-GW-RANAP-ACCESS-CLOSED schema. `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  
  Specifies the schema's format. `schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the [Schema Format String Length](#) on page 2013 section.

  For information on the schema format's syntax, see [Schema Format String Syntax](#) on page 2013.
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Important**

This command defines schemas used for RANAP messaging statistics collection in closed access mode. Multiple HNB-GW-RANAP-ACCESS-CLOSED schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the command using a different schema name.

**Usage Guidelines**

The following command creates a schema named `ranapclosed1stats1` that records the number of CS-Direct-Transfer messages sent and received on RANAP along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-ranap-access-closedschemaranapclosed1stats1 format "\%vpnname\%-\%vpnid\%-\%servname\%-\%cs-dir-transfer-rx\%-\%cs-dir-transfer-tx\%"
```

To create a schema named `ranapclosedpagingstats` that specifies a schema format of:

- Number of paging requests sent on RANAP from CS Core Network Connections: `cs-paging-req-tx`
- Number of paging requests sent on RANAP from PS Core Network Connections: `ps-paging-req-tx`

Use the following command:

```
hnbgw-ranap-access-closedschemaranapclosedpagingstats format "Number of paging requests sent on RANAP from CS Core Network Connections: %cs-paging-req-tx%
Number of paging requests sent on RANAP from PS Core Network Connections: %ps-paging-req-tx%"
```
hnbgw-ranap-access-hybrid schema

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.


**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

`hnbgw-ranap-access-hybrid schema schema_name format schema_format`

`no hnbgw-ranap-access-hybrid schema schema_name`

- **no**

  Removes the configured HNB-GW-RANAP-ACCESS-HYBRID schema.

  **schema_name**

  Specifies a name for the HNB-GW-RANAP-ACCESS-HYBRID schema. **schema_name** must be an alphanumeric string of 1 through 31 characters.

  **format schema_format**

  Specifies the schema's format.

  **schema_format** must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

  For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage Guidelines**

This command defines schemas used for RANAP messaging statistics collection in hybrid access mode. Multiple HNB-GW-RANAP-ACCESS-HYBRID schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-ranap-access-hybrid schema` `schema_name` command using a different schema name.

**Examples**

The following command creates a schema named `ranaphyb1stats1` that records the number of CS-Direct-Transfer messages sent and received on RANAP along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-ranap-access-hybrid schema ranaphyb1stats1 format
"%vpnname%%vpnid%-%servname%-%cs-dir-transfer-rx%-%cs-dir-transfer-tx%"
```

To create a schema named `ranaphypagingstats` that specifies a schema format of:

- Number of paging requests sent on RANAP from CS Core Network Connections: `cs-paging-req-tx`
- Number of paging requests sent on RANAP from PS Core Network Connections: `ps-paging-req-tx`

Use the following command:

```
hnbgw-ranap-access-hybrid schema ranaphypagingstats format "Number of paging requests sent on RANAP from CS Core Network Connections: %cs-paging-req-tx%\nNumber of paging requests sent on RANAP from PS Core Network Connections: %ps-paging-req-tx%"
```
hnbgw-ranap-access-open schema

---

**Important**

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures bulk statistics schema for Radio Access Network-Application Part (RANAP) message statistics collection in HNB-GW session instance for open access mode.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local] `host_name(config-bulkstats)#`

**Syntax Description**

- `hnbgw-ranap-access-open schema schema_name format schema_format`
- `no hnbgw-ranap-access-open schema schema_name`

**no**

Removes the configured HNB-GW-RANAP-ACCESS-OPEN schema.

**schema_name**

Specifies a name for the HNB-GW-RANAP-ACCESS-OPEN schema.

**schema_name** must be an alphanumeric string of 1 through 31 characters.

**format schema_format**

Specifies the schema's format.

**schema_format** must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.
For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage Guidelines**

This command defines schemas used for RANAP messaging statistics collection in open access mode. Multiple HNB-GW-RANAP-ACCESS-OPEN schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-ranap-access-open schema schema_name` command using a different schema name.

**Examples**

The following command creates a schema named `ranapopen1stats1` that records the number of CS-Direct-Transfer messages sent and received on RANAP along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-ranap-access-open schema ranapopen1stats1 format
"%vpnname%-%vpnid%-%servname%-%cs-dir-transfer-rx%-%cs-dir-transfer-tx%"
```

To create a schema named `ranapopenpagingstats` that specifies a schema format of:

- Number of paging requests sent on RANAP from CS Core Network Connections: `cs-paging-req-tx`
- Number of paging requests sent on RANAP from PS Core Network Connections: `ps-paging-req-tx`

Use the following command:

```
hnbgw-ranap-access-open schema ranapopenpagingtats format "Number of paging requests sent on RANAP from CS Core Network Connections: %cs-paging-req-tx% in Number of paging requests sent on RANAP from PS Core Network Connections: %ps-paging-req-tx%"
```

Command Line Interface Reference, Commands A - B, StarOS Release 20
hnbgw-rtp schema

**Important**

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.


**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
hnbgw-rtp schema schema_name format schema_format
no hnbgw-rtp schema schema_name
```

**no**

Removes the configured HNB-GW-RTP schema.

**schema_name**

Specifies a name for the HNB-GW-RTP schema.

**schema_name** must be an alphanumeric string of 1 through 31 characters.

**format schema_format**

Specifies the schema's format.

**schema_format** must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the [Schema Format String Length](#) on page 2013 section.

For information on the schema format's syntax, see [Schema Format String Syntax](#) on page 2013.
Usage Guidelines

This command defines schemas used for RTP messaging statistics collection. Multiple RTP schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-rtp schema schema_name` command using a different schema name.

Examples

The following command creates a schema named `rtp1stats1` that records the number of RTP uplink packets dropped and number of RTCP application report messages received on RTP link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rtp schema rtp1stats1 format
"%vpnname%-%vpnid%-%servname%-%rtp-uplink-pkts-dropped%-%rtcp-app-report-rx%"
```
**hnbgw-rtp-access-closed schema**

**Important**

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures bulk statistics schema for Real-Time Protocol (RTP) message statistics collection in HNB-GW session instance for closed access mode.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
hnbgw-rtp-access-closed schema schema_name format schema_format
no hnbgw-rtp-access-closed schema schema_name

no
```

Removes the configured HNB-GW-RTP-ACCESS-CLOSED schema.

```
schema_name
```

Specifies a name for the HNB-GW-RTP-ACCESS-CLOSED schema.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

```
format schema_format
```

Specifies the schema's format.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the [Schema Format String Length](#) on page 2013 section.

For information on the schema format's syntax, see [Schema Format String Syntax](#) on page 2013.
For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage Guidelines**

This command defines schemas used for RTP messaging statistics collection in closed access mode. Multiple HNB-GW-RTP-ACCESS-CLOSED schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-rtp-access-closed schema` command using a different schema name.

**Examples**

The following command creates a schema named `rtpclosed1stats1` that records the number of RTP uplink packets dropped and number of RTCP application report messages received on RTP link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rtp-access-closed schema rtpclosed1stats1 format
"%vpnname%-%vpnid%-%servname%-%rtp-uplink-pkts-dropped%-%rtcp-app-report-rx%"
```
**hnbgw-rtp-access-hybrid schema**

**Important**

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures bulk statistics schema for Real-Time Protocol (RTP) message statistics collection in HNB-GW session instance for hybrid access mode.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
hnbgw-rtp-access-hybrid schema schema_name format schema_format
no hnbgw-rtp-access-hybrid schema schema_name
```

**no**

Removes the configured HNB-GW-RTP-ACCESS-HYBRID schema.

**schema_name**

Specifies a name for the HNB-GW-RTP-ACCESS-HYBRID schema.

**schema_name** must be an alphanumeric string of 1 through 31 characters.

**format schema_format**

Specifies the schema's format.

**schema_format** must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.
Important

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage Guidelines

This command defines schemas used for RTP messaging statistics collection in hybrid access mode. Multiple HNB-GW-RTP-ACCESS-HYBRID schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-rtp-access-hybrid schema schema_name` command using a different schema name.

Examples

The following command creates a schema named `rtpphyb1stats1` that records the number of RTP uplink packets dropped and number of RTCP application report messages received on RTP link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rtp-access-hybrid schema rtpphyb1stats1 format "%vpnname%-%vpnid%-%servname%-%rtp-uplink-pkts-dropped%-%rtcp-app-report-rx%"
```
**hnbgw-rtp-access-open schema**

**Important**

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures bulk statistics schema for Real-Time Protocol (RTP) message statistics collection in HNB-GW session instance for open access mode.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
hnbgw-rtp-access-open schema schema_name format schema_format
no hnbw-gw-rtp-access-open schema schema_name
```

**no**

Removes the configured HNB-GW-RTP-ACCESS-OPEN schema.

**schema_name**

Specifies a name for the HNB-GW-RTP-ACCESS-OPEN schema.

**format schema_format**

Specifies the schema's format.

**schema_format** must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.
Important

For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage Guidelines**

This command defines schemas used for RTP messaging statistics collection in open access mode. Multiple HNB-GW-RTP-ACCESS-OPEN schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-rtp-access-open schema` command using a different schema name.

**Examples**

The following command creates a schema named `rtpopen1stats1` that records the number of RTP uplink packets dropped and number of RTCP application report messages received on RTP link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rtp-access-open schema rtpopen1stats1 format
"%vpnname%-%vpnid%-%servname%-%rtp-uplink-pkts-dropped%-rtcp-app-report-rx%"
```
hnbgw-rua schema

**Important**
In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures bulk statistics schema for RANAP User Adaptation (RUA) protocol message statistics collection in HNB-GW session instance.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

- `hnbgw-rua schema schema_name format schema_format`
- `no hnbgw-rua schema schema_name`

**no**
Removes the configured HNB-GW-RUA schema.

**schema_name**
Specifies a name for the HNB-GW-RUA schema.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**format schema_format**
Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the [Schema Format String Length](#), on page 2013 section.

For information on the schema format's syntax, see [Schema Format String Syntax](#), on page 2013.
Important
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage Guidelines
This command defines schemas used for RUA protocol messaging statistics collection. Multiple RUA schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-rua schema schema_name` command using a different schema name.

Examples
The following command creates a schema named `rua1stats1` that records the number of CS-Connect messages received and sent on RUA link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rua schema rua1stats1 format
"%vpnname%-%vpnid%-%servname%-%cs-connect-rx%-%cs-connect-tx%"
```
In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures bulk statistics schema for RANAP User Adaptation (RUA) protocol message statistics collection in HNB-GW session instance in closed access mode.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
hnbgw-rua-access-closed schema schema_name format schema_format
no hnbgw-rua-access-closed schema schema_name
```

**no**
Removes the configured HNB-GW-RUA-ACCESS-CLOSED schema.

**schema_name**
Specifies a name for the HNB-GW-RUA-ACCESS-CLOSED schema. `schema_name` must be an alphanumeric string of 1 through 31 characters.

**format schema_format**
Specifies the schema's format.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the [Schema Format String Length](#) on page 2013 section.

For information on the schema format's syntax, see [Schema Format String Syntax](#) on page 2013.
Important For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage Guidelines**

This command defines schemas used for RUA protocol messaging statistics collection in closed access mode. Multiple HNB-GW-RUA-ACCESS-CLOSED schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-rua-access-closed schema schema_name` command using a different schema name.

**Examples**

The following command creates a schema named `ruaclosed1stats1` that records the number of CS-Connect messages received and sent on RUA link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rua-access-closed schema ruaclosed1stats1 format "%vpnname%-%vpnid%-%servname%-%cs-connect-rx%-%cs-connect-tx%"
```
hnbgw-rua-access-hybrid schema

**Important**  
In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures bulk statistics schema for RANAP User Adaptation (RUA) protocol message statistics collection in HNB-GW session instance in hybrid access mode.

**Product**  
HNB-GW

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Bulk Statistics Configuration  
*configure > bulkstats mode*

Entering the above command sequence results in the following prompt:  

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
hnbgw-rua-access-hybrid schema schema_name format schema_format  
no hnbgw-rua-access-hybrid schema schema_name
```

**no**  
Removes the configured HNB-GW-RUA-ACCESS-HYBRID schema.

```
schema_name
```

Specifies a name for the HNB-GW-RUA-ACCESS-HYBRID schema.  
`schema_name` must be an alphanumeric string of 1 through 31 characters.

```
format schema_format
```

Specifies the schema's format.  
`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the [Schema Format String Length](#), on page 2013 section.  
For information on the schema format's syntax, see [Schema Format String Syntax](#), on page 2013.
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage Guidelines**

This command defines schemas used for RUA protocol messaging statistics collection in hybrid access mode. Multiple HNB-GW-RUA-ACCESS-HYBRID schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-rua-access-hyrbid schema` `schema_name` command using a different schema name.

**Examples**

The following command creates a schema named `ruahyb1stats1` that records the number of CS-Connect messages received and sent on RUA link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rua-access-hybrid schema ruahyb1stats1 format
"%vpnname%-%vpnid%-%servname%-%cs-connect-rx%-%cs-connect-tx%"
```
In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures bulk statistics schema for RANAP User Adaptation (RUA) protocol message statistics collection in HNB-GW session instance in open access mode.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

`Exec > Global Configuration > Bulk Statistics Configuration`

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
hnbgw-rua-access-open schema schema_name format schema_format
no hnbrgw-rua-access-open schema schema_name
```

`no`

Removes the configured HNB-GW-RUA-ACCESS-OPEN schema.

`schema_name`

Specifies a name for the HNB-GW-RUA-ACCESS-OPEN schema.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

`format schema_format`

Specifies the schema's format.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.
For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage Guidelines**

This command defines schemas used for RUA protocol messaging statistics collection in open access mode. Multiple HNB-GW-RUA-ACCESS-OPEN schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-rua-access-open schema schema_name` command using a different schema name.

**Examples**

The following command creates a schema named `ruaopen1stats1` that records the number of CS-Connect messages received and sent on RUA link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rua-access-open schema ruaopen1stats1 format ""%vpnname%-%vpnid%-%servname%-%cs-connect-rx%-%cs-connect-tx%"
```
**hnbgw-sctp schema**

<table>
<thead>
<tr>
<th>Important</th>
<th>In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.</th>
</tr>
</thead>
</table>


**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

`hnbgw-sctp schema schema_name format schema_format`

`no hnbgw-sctp schema schema_name`

- **no**
  
  Removes the configured SCTP schema.

- **schema_name**
  
  Specifies a name for the SCTP schema.

  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  
  Specifies the schema's format.

  `schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the [Schema Format String Length](#) on page 2013 section.

  For information on the schema format's syntax, see [Schema Format String Syntax](#) on page 2013.
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage Guidelines

This command defines schemas used for SCTP protocol messaging statistics collection. Multiple SCTP schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-sctp schema schema_name` command using a different schema name.

Examples

The following command creates a schema named `sctp1stats1` that records the number of bytes received from lower layer and number of bytes sent to lower layer over SCTP connection along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-sctp schema sctp1stats1 format
"%vpnname%-%vpnid%-%servname%-%total-bytes-sent-to-lower-layer%-%total-bytes-rcvd-from-lower-layer%"
```
**hsgw schema**

Configures HRPD Serving Gateway (HSGW) bulk statistics schema.

**Product**

HSGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local] host_name (config-bulkstats)#

**Syntax Description**

```plaintext
hsgw schema schema_name format schema_format
no hsgw schema schema_name
```

-no

Removes the specified schema.

**schema_name**

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**format schema_format**

Specifies the format of the collected HSGW statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

Use this command to define schemas for HSGW bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple HSGW schemas can be created to categorize HSGW bulk statistics. All of the schemas are processed at each collection interval. To create multiple HSGW schemas, re-issue the `hsgw schema schema_name` command using a different schema name each time.
**hss schema**

Configures Home Subscriber Service (HSS) bulk statistics schema.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Bulk Statistics Configuration
- configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
hss schema  schema_name  format  schema_format
no  hss schema  schema_name
```

**no**
Removes the specified schema.

**schema_name**
Specifies the schema's name.
- **schema_name** must be an alphanumeric string of 1 through 31 characters.

**format schema_format**
Specifies the schema's format.
- **schema_format** must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
- For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

---

**Important**
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

Use this command to define schemas for HSS bulk statistics collection. Multiple HSS schemas can be created to further categorize HSS bulk statistics. All of the schemas are processed at each collection interval. To create multiple HSS schemas, re-issue the `hss schema schema_name` command using a different schema name.

Examples

To create an hss schema named `hss_stats` that specifies a schema format of:

- Message Stats: Number of Cancel Location Request messages sent: `msg-cl-req`
- Message Stats: Number of Cancel Location Answer messages sent: `msg-cl-ans`

Use the following command:

```
hss schema hss_stats format "Message Stats: Number of Cancel Location Request messages sent: %msg-cl-req%\nMessage Stats: Number of Cancel Location Answer messages sent: %msg-cl-ans%\n"
```
icsr schema

Configures ICSR (Interchassis Session Recovery) bulkstats schema.

Product

All products that support ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax Description

icsr schema  schema_name  [ active-only ]  format  schema_format
no  icsr schema  schema_name

no

Deletes the named schema.

schema_name

Specifies the name of the schema as an alphanumeric string of 1 through 31 characters.

active-only

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

format schema_format

Specifies the schema's format.

schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

Important

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

Use this command to define schemas for ICSR bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple ICSR schemas can be created to categorize ICSR bulk statistics. All of the schemas are processed at each collection interval. To create multiple ICSR schemas, re-issue the `icsr schema schema_name` command using a different schema name each time.

You can also use this command to restrict the ICSR schema statistics to those gathered on the Active ICSR chassis.
imsa schema


**Product**
- GGSN
- HA
- HSGW
- IPSG
- PDSN
- P-GW
- S-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Bulk Statistics Configuration
- configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**
```
imsa schema  schema_name  [active-only]  format  schema_format
no  imsa schema  schema_name

no
Removes the specified schema.

schema_name
Specifies the schema's name.
schema_name must be an alphanumeric string of 1 through 31 characters.

active-only
Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.
```
**format schema_format**

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the **Schema Format String Length, on page 2013** section.

For information on the schema format's syntax, see the **Schema Format String Syntax, on page 2013** section.

---

**Important**

For a complete list of the statistics that are supported for this schema, refer to the **Statistics and Counters Reference**.

---

**Usage Guidelines**

Use this command to define schemas for IMSA bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple IMSA schemas can be created to categorize IMSA bulk statistics. All of the schemas are processed at each collection interval. To create multiple IMSA schemas, re-issue the **imsa schema schema_name** command using a different schema name each time.

You can also use this command to restrict the IMSA schema statistics to those gathered on the Active ICSR chassis.
ippool schema

Configures IP pool bulk statistics schema.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:
[local]host_name(config-bulkstats)#

Syntax Description

ippool schema schema_name [ active-only ] format schema_format
no ippool schema schema_name

no
Removes the specified schema.

schema_name
Specifies the schema's name.
schema_name must be an alphanumeric string of 1 through 31 characters.

active-only
Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

format schema_format
Specifies the schema's format.
schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

Important

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

Use this command to define schemas for IP pool bulk statistics collection. Multiple IP pool schemas can be created to further categorize 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 schema_name` command using a different schema name.

You can also use this command to restrict the IC IP pool schema statistics to those gathered on the Active ICSR chassis.

Examples

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

Configures IP Services Gateway (IPSG) bulk statistics schema.

**Product**

IPSG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local] *host_name*(config-bulkstats)#

**Syntax Description**

```
ipsg schema schema_name format schema_format
no ipsg schema schema_name
```

**no**

Removes the specified schema.

**schema_name**

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**format schema_format**

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

---

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

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 schema_name` command using a different schema name.

Examples

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 ippoolstats format "Context name: %vpnname%\nService name: %servname%\nTotal responses sent: %total-rsp-sent%\n"
```
lac schema

Configures LAC (L2TP Access Concentrator) bulk statistics schema.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

- **lac schema schema_name [active-only] format schema_format**
- **no lac schema schema_name**

no

Removes the specified schema.

schema_name

Specifies the schema's name.

schema_name must be an alphanumeric string of 1 through 31 characters.

active-only

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

format schema_format

Specifies the schema's format.

schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the **Schema Format String Length**, on page 2013 section.

For information on the schema format's syntax, see the **Schema Format String Syntax**, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the **Statistics and Counters Reference**.
Usage Guidelines

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 <schema_name>` command using a different schema name.

You can also use this command to restrict the LAC schema statistics to those gathered on the Active ICSR chassis.

Examples

The following command creates a schema named `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 named `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

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

`limit kilobytes`

**kilobytes**

Specifies the maximum amount of memory (in kilobytes) that may be used for bulk statistics as an integer from 1 through 32000. Default: 100

**Usage Guidelines**

Adjust bulk statics memory usage when considering the sampling interval adjustments.

**Caution**

Bulk statistics are stored in Random Access Memory (RAM) on the SPC/SMC/MIO. 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.

**Examples**

`limit 2048`
**link-aggr schema**

Configures Link Aggregation bulk statistic schema.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:
```
[local] host_name(config-bulkstats) #
```

**Syntax Description**
```
link-aggr schema  schema_name  [active-only]  format  schema_format
no link-aggr schema  schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema's name.
  *schema_name* must be an alphanumeric string of 1 through 31 characters.

- **active-only**
  Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

- **format schema_format**
  Specifies the schema's format.
  *schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section. For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

Use this command to define schemas for Link Aggregation bulk statistics collection. Multiple LMA service schemas can be created to categorize Link Aggregation service bulk statistics. All of the schemas are processed at each collection interval. To create multiple Link Aggregation service schemas, re-issue the `link-aggr schema schema_name` command using a different schema name.

You can also use this command to restrict the Link Aggregation schema statistics to those gathered on the Active ICSR chassis.
**Lma schema**

Configures the Local Mobility Anchor (LMA) statistics schema for the naming conventions of data files.

**Product**

P-GW
SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
lma schema schema_name [active-only] format schema_format
no lma schema schema_name
```

**no**

Removes the specified schema.

```
schema_name
```

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

```
active-only
```

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

```
format schema_format
```

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage Guidelines

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 schema_name` command using a different schema name.

You can also use this command to restrict the LMA schema statistics to those gathered on the Active ICSR chassis.

Examples

For an LMA-level schema named `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"
```
Ins schema

Configures LNS (L2TP Network Server) bulk statistics schema.

**Product**
LNS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax Description**

```
lns schema  schema_name  |  active-only  |  format  schema_format
no  lnsschema  schema_name
```

**no**
Removes the specified schema.

**schema_name**
Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**active-only**
Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

**format schema_format**
Specifies the format of the collected LNS statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.
Important

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage Guidelines

Use this command to define schemas for LNS bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple LNS schemas can be created to categorize LNS bulk statistics. All of the schemas are processed at each collection interval. To create multiple LNS schemas, re-issue the `ins schema schema_name` command using a different schema name each time.

You can also use this command to restrict the LNS schema statistics to those gathered on the Active ICSR chassis.
**mag schema**

Configures the Mobile Access Gateway (MAG) statistics schema for naming conventions of data files.

**Product**

HSGW  
S-GW  
SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration  
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
mag schema schema_name format schema_format  
no mag schema schema_name
```

**Syntax Description**

`no`

Removes the specified schema from MAG bulk statistics generation.

**schema_name**

Specifies the schema's name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

**format schema_format**

Specifies the schema's format.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

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 schema_name` command using a different schema name.

Examples

For a MAG-level schema named `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**

Configures MIPv6 HA (home Agent) bulk statistics schema.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
mipv6ha schema schema_name [ active-only ] format schema_format
no mipv6ha schema schema_name
```

no

Removes the specified schema.

```
schema_name
```

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

```
active-only
```

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

```
format schema_format
```

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the **Schema Format String Length**, on page 2013 section.

For information on the schema format's syntax, see the **Schema Format String Syntax**, on page 2013 section.

---

**Important**

For a complete list of the statistics that are supported for this schema, refer to the **Statistics and Counters Reference**.
Usage Guidelines

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` `schema_name` command using a different schema name.

You can also use this command to restrict the MIPv6 HA schema statistics to those gathered on the Active ICSR chassis.

Examples

The following command creates a schema named `mipv6haservicestats` that records the number of authorization attempt failures due to access rejects from AAA:

`mipv6ha schema mipv6haservicestats format "%%aaa-actauthfail\""`
mme schema

Configures MME (Mobility Management Entity) bulk statistics schema.

**Product:** MME

**Privilege:** Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

```configure > bulkstats mode```

Entering the above command sequence results in the following prompt:

```
[local] <host_name> (config-bulkstats)#
```

**Syntax Description**

```mme schema  schema_name  [active-only]  format  schema_format
no mme schema  schema_name
```

**no**

Removes the specified schema.

**schema_name**

Specifies the schema's name.

- `schema_name` must be an alphanumeric string of 1 through 31 characters.

**active-only**

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

**format schema_format**

Specifies the schema's format.

- `schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

---

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

Use this command to define schemas for MME bulk statistics collection. Multiple MME bulk statistics schemas can be created to categorize MME bulk statistics. All of the schemas are processed at each collection interval. To create multiple MME service schemas, re-issue the `mme schema schema_name` command using a different schema name.

You can also use this command to restrict the MME schema statistics to those gathered on the Active ICSR chassis.

Examples

The following command creates a schema named `mmeservice_s1ap_cfg_transfers` that records the total number of S1AP - transmit data - configuration transfers:

```
mme schema mmeservice_s1ap_cfg_transfers format "s1ap-trnsdata-cfg-tfr"
```
mvs schema

Configures MVS (Mobile Videoscape) bulk statistics schema.

**Important**

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

- `mvs schema schema_name [active-only] format schema_format`
- `no mvs schema schema_name`

`no`

Removes the specified schema.

`schema_name`

Specifies the schema's name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

`active-only`

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

`format schema_format`

Specifies the schema's format.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the [Schema Format String Length](#) on page 2013 section.

For information on the schema format's syntax, see the [Schema Format String Syntax](#) on page 2013 section.
Important

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage Guidelines

Use this command to define schemas for MVS bulk statistics collection. Multiple LMA service schemas can be created to categorize MVS bulk statistics. All of the schemas are processed at each collection interval. To create multiple MVS schemas, re-issue the `mvs schema schema_name` command using a different schema name.

You can also use this command to restrict the MVS schema statistics to those gathered on the Active ICSR chassis.
nat-realm schema

Creates and configures Network Address Translation (NAT) realm statistics schema.

**Product**  
NAT

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Bulk Statistics Configuration  
  
```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats) #
```

**Syntax Description**

```
nat-realm schema  schema_name  format  schema_format
no nat-realm schema  schema_name
```

**schema_name**

Specifies the schema's name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

**format  schema_format**

Specifies the schema's format.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

---

**Important**  
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage Guidelines**

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  schema_name` command using a different schema name.
The following command creates a NAT realm schema with the VPN name, realm name, and flows information:

```
nat-realm schema realm1 format "%%vpnname%% %realmname%% %nat-rlm-flows%%"
```
**p2p schema**

Creates and configures P2P (Peer-to-Peer) statistics schema.

**Product**
ADC

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats) #
```

**Syntax Description**

```
p2p schema schema_name | active-only | format schema_format
no p2p schema schema_name
```

- **schema_name**
  Specifies the schema's name.
  - *schema_name* must be an alphanumeric string of 1 through 31 characters.

- **active-only**
  Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

- **format schema_format**
  Specifies the schema's format.
  - *schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
  - For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
**Usage Guidelines**

Use this command to define schemas for P2P bulk statistics collection. Multiple P2P schemas can be created to further categorize P2P-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple P2P schemas, re-issue the `p2p schema schema_name` command using a different schema name.

You can also use this command to restrict the P2P schema statistics to those gathered on the Active ICSR chassis.

**Examples**

The following command creates a schema named `p2pstats` to record the total number of bytes detected in uplink and downlink direction:

```
p2p schema p2pstats format "\%p2p-uplnk-bytes-name\%\%p2p-uplnk-bytes-value\%\%p2p-dwlnk-bytes-name\%\%p2p-dwlnk-bytes-value\%"
```
pcc-af schema

Configures Policy and Charging Control-Application Function (PCC-AF) service bulk statistics schema.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax Description**

`pcc-af schema schema_name format schema_format`

`no pcc-af schema schema_name`

`no`

Removes the specified schema.

`schema_name`

Specifies the schema’s name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

`format schema_format`

Specifies the schema's format.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format’s syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
**Usage Guidelines**

Use this command to define schemas for PCC-AF service bulk statistics collection. Multiple PCC-AF service schemas can be created to categorize PCC-AF service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PCC-AF service schemas, re-issue the `pcc-af schema schema_name` command using a different schema name.

**Examples**

The following command creates a schema named `pcc_af1stats1` that records the total number of Rx STR messages received and total number of Rx AAR Accept messages sent along with Context name, Context Id, and PCC-AF service name:

```
pcc-af schema pcc_af1stats1 format
"%vpnname%-%vpnid%-%servname%-%total-rx-ccai-accept-sent%-%total-rx-aar-accept-sent%"
```
**pcc-policy schema**

Configures Policy and Charging Control-Policy (PCC-Policy) service bulk statistics schema.

**Product**  
IPCF

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Bulk Statistics Configuration

```text
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```text
[local] host_name(config-bulkstats) #
```

**Syntax Description**  

```text
pcc-policy schema schema_name format schema_format  
nopcc-policy schema schema_name
```

**no**  
Removes the specified schema.

**schema_name**  
 Specifies the schema's name.

**schema_name** must be an alphanumeric string of 1 through 31 characters.

**format schema_format**  
 Specifies the schema's format.

**schema_format** must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**  
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
**Usage Guidelines**

Use this command to define schemas for PCC-Policy service bulk statistics collection. Multiple PCC-Policy service schemas can be created to categorize PCC-Policy service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PCC-Policy service schemas, re-issue the `pcc-policy schema schema_name` command using a different schema name.

**Examples**

The following command creates a schema named `pcc_plcy1stats1` that records the total number of Gx messages sent and total number of Gx CCR messages received along with Context name, Context Id, and PCC-Policy service name:

```
pcc-policy schema pcc_plcy1stats1 format
"%vpnname%-%vpnid%-%servname%-%total-gx-outbound-msgs%-%total-gx-ccr-rcvd%"
```
**pcc-profile schema**

Configures Policy and Charging Control Profile (PCC-Profile) bulk statistics schema.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

**configure > bulkstats mode**

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats) #
```

**Syntax Description**

```
pcc-profile schema schema_name format schema_format
no pcc-profile schema schema_name
```

**no**

Removes the specified schema.

**schema_name**

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**format schema_format**

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

Use this command to define schemas for PCC-Profile bulk statistics collection. Multiple PCC-Profile schemas can be created to categorize PCC-Profile bulk statistics. All of the schemas are processed at each collection interval. To create multiple PCC-Profile schemas, re-issue the `pcc-profile schema schema_name` command using a different schema name.

Examples

The following command creates a schema named `pcc_profile1stats1` that records the total number of SGSN changes and QoS changes occurred for particular PCC profile along with Context name, Context Id, and PCC-Service name:

```
pcc-profile schema pcc_profile1stats1 format
"%vpnname%-%vpnId%-%servname%-%total-sgsn-change%-%total-qos-change%"
```
pcc-sp-endpt schema

Configures the bulkstats schema at the Sp interface endpoint for PCC procedures with Subscriber Service Controller/Subscriber Policy Register (SSC/SPR).

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration

**Syntax Description**

```plaintext
pcc-sp-endpt schema schema_name format schema_format  
nopcc-sp-endpt schema schema_name

no
```

Removes the specified schema.

**schema_name**
Specifies the schema's name.

**format schema_format**
Specifies the schema's format.

**Important**
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
**Usage Guidelines**

Use this command to define schemas for PCC-Sp-Endpoint bulk statistics collection. Multiple PCC-Sp-Endpoint schemas can be created to categorize PCC-Sp-Endpoint bulk statistics. All of the schemas are processed at each collection interval. To create multiple PCC-Sp-Endpoint schemas, re-issue the `pcc-sp-endpt schema schema_name` command using a different schema name.

**Examples**

The following command creates a schema named `pcc_sp1stats1` that records the total number of SPRMgr Sh session close and open requests received from PCCMgr and processed by PCC-Sp-Endpoint along with Context name, Context Id, and PCC-Sp-Endpoint name:

```
pcc-sp-endpt schema pcc_svc1stats1 format
"%vpnname%-%vpnid%-%endpt-name%-%req-open%-%req-close%"
```
**pcc-service schema**

Configures Policy and Charging Control-Service (PCC-Service) bulk statistics schema.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

```plaintext
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```plaintext
[local]\host_name\(config-bulkstats)#
```

**Syntax Description**

```plaintext
pcc-service schema schema_name format schema_format
no pcc-service schema schema_name
```

**no**

Removes the specified schema.

```plaintext
schema_name
```

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

```plaintext
format schema_format
```

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

Use this command to define schemas for PCC-Service bulk statistics collection. Multiple PCC-Service schemas can be created to categorize PCC-Service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PCC-Service schemas, re-issue the `pcc-service schema schema_name` command using a different schema name.

Examples

The following command creates a schema named `pcc_svc1stats1` that records the total number of Gx and Gy request processed by PCC-Service along with Context name, Context Id, and PCC-Service name:

```
pcc-service schema pcc_svc1stats1 format
"%vpnname%-%vpnid%-%servname%-%total-gx-processed%-%total-gy-processed%"
```
pdif schema

Configures Packet Data Interworking Function (PDIF) bulk statistics schema.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration

```text
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats) #
```

**Syntax Description**

```text
pdif schema schema_name format schema_format
no pdif schema schema_name
```

**no**
Removes the specified schema.

```text
schema_name
```
Specifies the schema's name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

**format schema_format**
Specifies the schema's format.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

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 schema_name` command using a different schema name.

Examples

The following command creates a schema named `pdifschema1` for the category current active ipv4 sessions:

```
pdif schema pdifschema1 format %sess-curactip4%
```
pgw schema

Configures Packet Data Network Gateway (P-GW) bulk statistics schema.

**Product**

- P-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
pgw schema schema_name [active-only] format schema_format
no pgw schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema's name.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **active-only**
  Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

- **format schema_format**
  Specifies the schema's format.
  `schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
  For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.
Usage Guidelines

Use this command to define schemas for P-GW bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple P-GW schemas can be created to categorize P-GW bulk statistics. All of the schemas are processed at each collection interval. To create multiple P-GW schemas, re-issue the `pgw schema schema_name` command using a different schema name each time.

You can also use this command to restrict the P-GW schema statistics to those gathered on the Active ICSR chassis.
port schema

Configures port bulk statistics schema.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
port schema schema_name  [active-only] format schema_format
no port schema schema_name
```

**no**

Removes the specified schema.

**schema_name**

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**active-only**

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

**format schema_format**

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

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 schema_name` command using a different schema name.

You can also use this command to restrict the port schema statistics to those gathered on the Active ICSR chassis.

Important

The `card` variable in the Port schema is not supported on all platforms

Examples

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**

Configures Point-to-Point Protocol (PPP) bulk statistics schema.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration  
`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-bulkstats) #
```

**Syntax Description**

```
ppp schema  schema_name  [active-only]  format  schema_format  
no  ppp schema  schema_name
```

**no**

Removes the specified schema.

**schema_name**

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**active-only**

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

**format schema_format**

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the **Schema Format String Length**, on page 2013 section.

For information on the schema format's syntax, see the **Schema Format String Syntax**, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the **Statistics and Counters Reference**.
Usage Guidelines
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 schema_name` command using a different schema name.

You can also use this command to restrict the PPP schema statistics to those gathered on the Active ICSR chassis.

Examples
To create a ppp-level schema named `pppstats` that specifies a schema format of:
- CHAP: (Challenge Handshake Authentication Protocol)
- PAP: (Password Authentication Protocol)

Use the following command:
`ppp schema pppstats format "CHAP:
Auth. Attempts: %auth-attempt-chap%\tAuth. Successes: %auth-success-chap%
PAP:
Auth. Attempts: %auth-attempt-pap%\tAuth. Successes: %auth-success-pap%"`
ps-network-gtpu schema

Important
In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures the GTP-U bulk statistics schema in a Packet Switched (PS) network associated with an HNB-GW node.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:
[local]\host_name\(config-bulkstats)\#n

Syntax Description
ps-network-gtpu schema schema_name format schema_format
no ps-network-gtpu schema schema_name

no
Removes the specified schema.

schema_name
Specifies the schema's name.
schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format
Specifies the schema's format.
schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.
Important

For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage Guidelines**

Use this command to define schemas for GTP-U connection related bulk statistics collection in a PS network associated with HNB-GW in a Femto UMTS network. Multiple PS Networks GTP-U schemas can be created to further categorize at PS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple PS Networks GTPU schemas, re-issue the `ps-network-gtpu schema schema_name` command using a different schema name.

**Examples**

The following command creates a schema named `ps_gtpu1stats1` that records the total number of GTP-U packets received by HNB-GW from CN and sent to CN node in an associated PS network:

```
ps-network-gtpu schema ps_gtpu1stats1 format "%gtpu-pkt-rx%" "%gtpu-pkt-tx%"
```
ps-network-ranap schema

---

**Important**
In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

---


**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
ps-network-ranap schema  schema_name  format  schema_format
no  ps-network-ranap schema  schema_name
```

**no**
Removes the specified schema.

```
schema_name
```
Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

```
format  schema_format
```
Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.
For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage Guidelines**

Use this command to define schemas for RANAP procedure related bulk statistics collection in a PS network associated with HNB-GW in a Femto UMTS network. Multiple PS Networks RANAP schemas can be created to further categorize at PS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple PS Networks RANAP schemas, re-issue the `ps-network-ranap schema schema_name` command using a different schema name.

**Examples**

The following command creates a schema named `ps_ranap1stats1` that records the total number of Iu Release Request messages transmitted and total number of Iu Release Command message received by HNB-GW node:

```
ps-network-ranap schema ps_ranap1stats1 format "%iul-rel-req-tx%" "%iul-rel-cmd-rx%"
```
ps-network-sccp schema

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures the Signalling Connection Control Part (SCCP) bulk statistics schema in a Packet Switched (PS) network associated with an HNB-GW node.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration
```
configure > bulkstats mode
```
Entering the above command sequence results in the following prompt:
```
[local]host_name(config-bulkstats)#
```

**Syntax Description**
```
ps-network-sccp schema schema_name format schema_format
no ps-network-sccp schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema's name.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the schema's format.
  `schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
  For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.
For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage Guidelines**

Use this command to define schemas for SCCP connection related bulk statistics collection in a PS network associated with HNB-GW in a Femto UMTS network. Multiple PS Networks SCCP schemas can be created to further categorize at PS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple PS Networks SCCP schemas, re-issue the `ps-network-sccp schema schema_name` command using a different schema name.

**Examples**

The following command creates a schema named `ps_sccplstats1` that records the total number of SCCP connection requests received by HNB-GW and responses sent to CN node in an associated PS network: `ps-network-sccp schema ps_sccplstats1 format "%sccp-conn-req-rx%" "%sccp-conn-req-tx%"`
radius schema

Configures RADIUS bulk statistics schema.

Product

PDSN
GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax Description

radius schema schema_name [active-only] format schema_format
no radius schema schema_name

no

Removes the specified schema.

schema_name

Specifies the schema's name.

schema_name must be an alphanumeric string of 1 through 31 characters that is case sensitive.

active-only

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

format schema_format

Specifies the schema's format.

schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.
Important

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage Guidelines

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 schema_name` command using a different schema name.

You can also use this command to restrict the RADIUS schema statistics to those gathered on the Active ICSR chassis.

Examples

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%\nAuthentication Requests Sent: %auth-req-sent%\nAccounting Requests Sent: %acc-req-sent%"
```
radius-group schema

Configures RADIUS group bulk statistics schema.

Product

PDSN
GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]<host_name>(config-bulkstats)#

Syntax Description

radius-group schema  schema_name  [active-only]  format  schema_format
no radius-group schema  schema_name

no

Removes the specified schema.

schema_name

Specifies the schema's name.
schema_name must be an alphanumeric string of 1 through 31 characters that is case sensitive.

active-only

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

format schema_format

Specifies the schema's format.
schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.
For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage Guidelines**

Use this command to define schemas for RADIUS group bulk statistics collection. Multiple RADIUS group schemas can be created to categorize RADIUS group bulk statistics. All of the schemas are processed at each collection interval. To create multiple RADIUS group schemas, re-issue the `radius-group schema schema_name` command using a different schema name.

You can also use this command to restrict the RADIUS group schema statistics to those gathered on the Active ICSR chassis.

**Examples**

To create a RADIUS group 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-group schema radius_statistics format "Server: %ipaddr%\nAuthentication Requests Sent: %auth-req-sent%\nAccounting Requests Sent: %acc-req-sent%"
```
**receiver**

Configures a host system to receive bulk stats information through Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP) or SSH File Transfer Protocol (SFTP).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

*configure > bulkstats mode*

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax Description**

```
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 bulk stats 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 is not currently 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 using 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 alphanumeric string of 1 through 31 characters. The password to use for remote system authentication is specified as pwd and must be from 1 to 31 characters or 1 to 64 characters if the encrypted keyword is also specified.

sftp login user_name [ encrypted ] password pwd: the SFTP protocol shall be used for data file transfer.
user_name specifies the user to provide for remote system secure logins and must be an alphanumeric string of 1 through 31 characters. The password to use for remote system authentication is specified as pwd and must be from 1 to 31 characters or 1 to 64 characters if the encrypted keyword is also specified.

tftp: the TFTP protocol is to be used to transfer files.
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 Guidelines
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 receiver. If the primary receiver is unreachable for any reason, the secondary receiver is used. If the secondary receiver is also unreachable, the system retries after a delay period where it again attempts to connect to the primary receiver followed by the secondary receiver 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.

Examples
receiver 10.2.3.4 primary mechanism tftp
receiver 10.2.3.5 secondary
no receiver 10.2.3.4
**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

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax Description**

Remotefile format schema_format [ both-receivers | primary-receiver | secondary-receiver ]

no remotefile format

no

 Resets the remote file naming convention to the system default.

format schema_format

Specifies the naming convention format to use.

schema_format must be an alphanumeric string of 1 through 127 characters. The format string syntax is described in the [Schema Format String Syntax](#) on page 2013 section. Default: "%date%-%time%"

**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 23: remote file Command Naming Format Variables**

<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>Variable</td>
<td>Description</td>
<td>Data Type</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>-----------</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**

Sets the remote file creation target to both receivers, primary receiver or secondary receiver. Default: Both receivers.

**Usage Guidelines**

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 specifies 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 it has not yet been transferred.

**Examples**

```
remotefile format simpleFormat
remotefile format ""%host%-%date%-%time%"
remotefile format ""%host%-%date%-%time%" both-receivers
remotefile format ""%host%-%date%"" primary-receiver
no remotefile format
```
**rlf schema**

Configures the aggregated information for Rate Limiting Function (RLF) context statistics schema.

**Product**
- GGSN
- P-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**

`Exec > Global Configuration > Bulk Statistics Configuration`

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats) #
```

**Syntax Description**

- `rlf schema schema_name format schema_format`
- `no rlf schema schema_name`

**no**

Removes the specified schema.

**schema_name**

Specifies the schema's name.

- `schema_name` must be an alphanumeric string of 1 through 31 characters.

**format schema_format**

Specifies the schema's format.

- `schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the `Schema Format String Length`, on page 2013 section.

For information on the schema format's syntax, see the `Schema Format String Syntax`, on page 2013 section.

---

**Important**

For a complete list of the statistics that are supported for this schema, refer to the `Statistics and Counters Reference`. 
Usage Guidelines

Use this command to define schemas for RLF bulk statistics collection. Multiple RLF schemas can be created to categorize RLF bulk statistics. All of the schemas are processed at each collection interval. To create multiple RLF schemas, re-issue the `rlf schema schema_name` command using a different schema name.

Examples

To create an RLF-level schema named `rlfstats` that specifies a schema format of:

- Date: `date`
- Time: `time`
- Number of Authentication Denials: `deny-auth`

Use the following command:

```
rlf schema rlfsstats format "Date: %date%\nTime: %time%\nNumber of Authentication Denials: %deny-auth%\n"
```
rlf-detailed schema

Configures the detailed instance level information for RLF context statistics schema.

**Product**
- GGSN
- P-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Bulk Statistics Configuration
  - configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-bulkstats) #
```

**Syntax Description**

```
rlf-detailed schema schema_name format schema_format
no rlf-detailed schema schema_name
```

**no**
Removes the specified schema.

**schema_name**
Specifies the schema's name.

- **Important**
  - For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**schema_name** must be an alphanumeric string of 1 through 31 characters.

**format schema_format**
Specifies the schema's format.

- **Important**
  - For more information, see the *Schema Format String Length*, on page 2013 section.
  - For information on the schema format's syntax, see the *Schema Format String Syntax*, on page 2013 section.

- **schema_format** must be a string of 1 through 3599 characters, including spaces within double quotation marks (" ").
Usage Guidelines

Use this command to define schemas for detailed RLF bulk statistics collection. Multiple rlf-detailed schemas can be created to categorize RLF detailed bulk statistics. All of the schemas are processed at each collection interval. To create multiple rlf-detailed schemas, re-issue the `rlf-detailed schema schema_name` command using a different schema name.

Examples

To create an rlf-detailed level schema named `rlfdetailedstats` that specifies a schema format of:

- Date: `date`
- Time: `time`
- Number of Authentication Denials: `deny-auth`

Use the following command:

```
rlf-detailed schema rlfstats format "Date: %date%\nTime: %time%\nNumber of Authentication Denials: %deny-auth%\n"
```
**rp schema**

Configures R-P bulk statistics schema.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
rp schema schema_name [ active-only ] format schema_format
no rp schema schema_name
```

**no**

Removes the specified schema.

**schema_name**

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**active-only**

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

**format schema_format**

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

---

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

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 schema_name` command using a different schema name.

You can also use this command to restrict the R-P schema statistics to those gathered on the Active ICSR chassis.

Examples

To create an PDSN-level schema named `pdsn servicestats` that specifies a schema format of:

- Date: `date`
- Time: `time`
- Number of Authentication Denials: `deny-auth`

Use the following command:

```bash
rp schema rpservicestats format "Date: %date%\nTime: %time%\nNumber of Authentication Denials: %deny-auth%\n"
```
saegw schema

Configures System Architecture Evolution Gateway (SAEGW) bulk statistics schema.

**Product**
SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
saegw schema  [active-only] format schema_format
no saegw schema schema_name
```

**no**
Removes the specified schema.

```
schema_name
```
Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

```
active-only
```
Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

```
format schema_format
```
Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

Use this command to define schemas for SAEGW bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple SAEGW schemas can be created to categorize SAEGW bulk statistics. All of the schemas are processed at each collection interval. To create multiple SAEGW schemas, re-issue the `saegw schema schema_name` command using a different schema name each time.

You can also use this command to restrict the SAEGW schema statistics to those gathered on the Active ICSR chassis.
sample-interval

Configures the time interval between collecting local statistics.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration
```
configure > bulkstats mode
```
Entering the above command sequence results in the following prompt:
```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
sample-interval minutes
```

*minutes*
Specifies the frequency (in minutes) of polling for local statistics as an integer from 1 through 1440.

**Usage Guidelines**
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.

**Examples**
sample-interval 120
sbc schema

Configures the collection of statistics for the SBe schema.

Product
MME

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:
[local]host_name(config-bulkstats)#

Syntax Description
sbc schema  schema_name  format  schema_format
no  sbc schema  schema_name

no
Removes the specified SBe schema from statistics collection.

schema_name
Specifies the schema's name.
schema_name must be an alphanumeric string of 1 through 31 characters.

format  schema_format
Specifies the schema's format.
schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.
For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

Important
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

Use this command to define schemas for SBc bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple SBc schemas can be created to categorize SBc bulk statistics. All of the schemas are processed at each collection interval. To create multiple SBc schemas, re-issue the `sbc schema schema_name` command using a different schema name each time.

Examples

Include the bulk statistic variable names to create an SBc schema named `stats_SBc_pkts_tx_rx` that specifies a collection of statistics (a schema format). The following command defines the collection of the total number of SCTP packets transmitted and received:

```
sbc schema stats_SBc_pkts_tx_rx format "Total SCTP Packets Sent: %sctp-totsent-pkts\nTotal SCTP Packets Received: %sctp-totrec-pkts\n"
```
**sccp schema**

**Important**

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

Configures the collection of statistics for the SCCP schema.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

**configure** > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax Description**

`sccp schema schema_name format schema_format

no sccp schema schema_name

no`  

Removes the specified schema.

`schema_name`

Specifies the schema's name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

`format schema_format`

Specifies the schema's format.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see Schema Format String Syntax, on page 2013.
For a complete list of the statistics that are supported for the SCCP schema, refer to the *Statistics and Counters Reference*.

**Usage Guidelines**

Use this command to define schemas for SCCP bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple SCCP schemas can be created to categorize SCCP bulk statistics. All of the schemas are processed at each collection interval. To create multiple SCCP schemas, re-issue the `sccp schema schema_name` command using a different schema name each time.

**Examples**

Include the bulk statistic variable names to create an SCCP schema named `sccpstats11` that specifies collection of statistics (a schema format) for:

- Subsystem available messages sent from the SCCP
- Subsystem available messages received by the SCCP

Use the following command:

```
  sccp schema sccpstats11 format "Subsys avail SCCP Tx: %ssa-txed\nSubsys avail SCCP Rx: %ssa-rcvd\n"
```
**schema**

Configures the system-level bulk statistics schema.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax Description**

- `schema schema_name [active-only] format schema_format`
- `no schema schema_name`

- `no`
  Removes the specified schema.

- `schema_name`
  Specifies the schema's name.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- `active-only`
  Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

- `format schema_format`
  Specifies the schema's format.
  `schema_format` must be an alphanumeric string of 1 through "1021 minus "number of characters in rest of the command, including spaces"" characters. For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage Guidelines**

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 schema_name` command using a different schema name.

You can also use this command to restrict the schema statistics to those gathered on the Active ICSR chassis.

**Examples**

The following command creates a schema named `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 named `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"
```
**sgs schema**

Configures the collection of statistics for the SGs interface schema.

**Product**  MME

**Privilege**  Security Administrator, Administrator

**Command Modes**  Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sgs schema schema_name [active-only] format schema_format</code></td>
<td>Configures the SGs schema.</td>
</tr>
<tr>
<td><code>no sgs schema schema_name</code></td>
<td>Removes the specified SGs schema from statistics collection.</td>
</tr>
</tbody>
</table>

`schema_name`

Specifies the schema's name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

`active-only`

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

`format schema_format`

Specifies the schema's format.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the [Schema Format String Length](#), on page 2013 section.

For information on the schema format's syntax, see the [Schema Format String Syntax](#), on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*. 
Usage Guidelines

Use this command to define schemas for SGs bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple SGs schemas can be created to categorize SGs bulk statistics. All of the schemas are processed at each collection interval. To create multiple SGs schemas, re-issue the `sgs schema schema_name` command using a different schema name each time.

You can also use this command to restrict the SGs schema statistics to those gathered on the Active ICSR chassis.

Examples

Include the bulk statistic variable names to create an SGs schema named `stats_SGs_release` that specifies a collection of statistics (a schema format) for the total number of release messages transmitted, retransmitted, and received:

Use the following command:

```
sgs schema stats_SGs_release format "Total transmitted: %rel-req-tx\nTotal retransmitted: %rel-req-retx\nTotal received: %rel-req-rx\n"
```
**sgs-vlr schema**

Configures the collection of statistics for the SGs-VLR schema.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
sgs-vlr schema  schema_name  [active-only]  format  schema_format
no  sgs schema  schema_name

no
```

Removes the specified SGs-VLR schema from statistics collection.

```
schema_name
```

Specifies the schema's name.

```
schema_name
```

must be an alphanumeric string of 1 through 31 characters.

```
active-only
```

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

```
format  schema_format
```

Specifies the schema's format.

```
schema_format
```

must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

---

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

Use this command to define schemas for SGs-VLR bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple SGS-VLR schemas can be created to categorize SGS-VLR bulk statistics. All of the schemas are processed at each collection interval. To create multiple SGS-VLR schemas, re-issue the `sgs-vlr schema schema_name` command using a different schema name each time.

You can also use this command to restrict the SGs-VLR schema statistics to those gathered on the Active ICSR chassis.

Examples

Include the bulk statistic variable names to create an SGs-VLR schema named `stats_SGsVLR_release` that specifies a collection of statistics (a schema format) for the total number of release messages transmitted, retransmitted, and received:

Use the following command:

```bash
sgs-vlr schema stats_SGsVLR_release format "Total Paging requests transmitted: %pag-req-tx%\nTotal Paging requests retransmitted: %pag-req-retx%\nTotal Paging requests received: %pag-req-rx%"
```
sgsn schema

Configures the collection of statistics for the SGSN schema.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax Description

sgsn schema schema_name format schema_format

no sgsn schema schema_name

no

Removes the specified SGSN schema from statistics collection.

schema_name

Specifies the schema's name.

schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format

Specifies the schema's format.

schema_format must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

Important For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
**Usage Guidelines**

Use this command to define schemas for SGSN bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple SGSN schemas can be created to categorize SGSN bulk statistics. All of the schemas are processed at each collection interval. To create multiple SGSN schemas, re-issue the `sgsn schema schema_name` command using a different schema name each time.

**Examples**

Include the bulk statistic variable names to create an SGSN schema named `stats_3Gsgsn1` that specifies collection of statistics (a schema format) for the total number of 3G Attaches per LAC/RAC per MCC & MNC:

Use the following command:

```
sgsn schema stats_3Gsgsn1 format "MCC: %mcc\nMNC: %mnc\nLAC: %lac\nRAC: %rac\nTotal 3G Subs Attached: %3G-attached\n"
```
sgtp schema

Configures the collection of the SGSN's GTP-C and GTP-U activity statistics.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax Description**

- `sgtp schema schema_name format schema_format`
- `no sgtp schema schema_name`

`no`  
Removes the specified SGTP schema from statistics collection.

`schema_name`  
Specifies the schema's name.  
`schema_name` must be an alphanumeric string of 1 through 31 characters.

`format schema_format`  
Specifies the schema's format.  
`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**  
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

Use this command to define schemas for SGTP bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple SGTP schemas can be created to categorize SGTP bulk statistics. All of the schemas are processed at each collection interval. To create multiple SGTP schemas, re-issue the `sgtp schema schema_name` command using a different schema name each time.

Examples

Include the bulk statistic variable names to create an SGTP schema named `sgtpstats_sgsn1` that specifies collection of statistics (a schema format) will be by IuPS service interface and by RNC for the total number of GTP-C Create PDP Context Request messages received.

Use the following command:

```
sgtp schema sgtpstats_sgsn1 format "IuPS Service ID: %iups-service%
RNC: %rnc-address%
Total CPC Rx: %sgtpc-total-cpc-req%"
```
**sgw schema**

Configures the collection of the S-GW activity statistics.

**Product**

S-GW
SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```
sgw schema schema_name format schema_format
no sgw schema schema_name
```

- **no**
  Removes the specified S-GW schema from statistics collection.

- **schema_name**
  Specifies the schema's name.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the schema's format.
  `schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the *Schema Format String Length*, on page 2013 section.
  For information on the schema format's syntax, see the *Schema Format String Syntax*, on page 2013 section.

---

**Important**

For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*. 
Usage Guidelines

Use this command to define schemas for S-GW bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple S-GW schemas can be created to categorize S-GW bulk statistics. All of the schemas are processed at each collection interval. To create multiple S-GW schemas, re-issue the `sgw schema schema_name` command using a different schema name each time.

Examples

Include the bulk statistic variable names to create an S-GW schema named `sgwstats_sgw1` that specifies collection of statistics (a schema format) will be by S-GW service interface for the total number of currently idle and active UEs.

Use the following command:

```
sgw schema sgwstats_sgw1 format "SGW Service ID: %servname%
Total Current Idle UEs: %sessstat-totcur-ueidle%
Total Current Active UEs: %sessstat-totcur-ueactive%"
```

show variables

Displays the bulk statistics variable information based on schema names.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:
[local]host_name(config-bulkstats)#

Syntax Description
show variables [schema_name] [obsolete]

show variables schema_name
Displays all valid bulkstat schema statistics, or only the statistics for the specified schema.

schema_name specifies the name of the schemas available on the system. Following is the list of available schemas in this release.

- aal2
- alcap
- apn
- asngw
- asnpc
- bcmcs
- card
- closedrp
- common
- context
- cs-network-ranap
- cs-network-rtp
- dcca
In Release 20.0, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.
In Release 20.0, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

- hsgw
- imsa
- ippool
- ipsg
- lac
- lma
- lns
- mag
- map
- mipv6ha
- mme
- mvs
- nat-realm
- p2p
- pcc-af
- pcc-policy
- pcc-quota
- pcc-service
- pcc-sp-endpt
- pdg
- pdif
- pgw
- phsgw
- phspc
- port
- ppp
- ps-network-ranap
- radius
- radius-group
- rlf


- rlf-detailed
- rp
- saegw
- sccp
- sgs
- sgsn
- sgtp
- sgw
- ss7link
- ss7rd
- system
- vpn

**obsolete**

Displays obsolete (but still available) schema variables. An asterisk (*) is displayed next to schema variables that have been obsoleted.

**Usage Guidelines**

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.

**Examples**

The following command displays the bulkstat variables only for the card schema:

```
show variables card
```
**sles schema**

Configures the collection of statistics for the SLs interface schema.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax Description**

`sle schema schema_name format schema_format`

`no sle schema schema_name`

`no`

Removes the specified SLs schema from statistics collection.

`schema_name`

Specifies the schema's name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

`format schema_format`

Specifies the schema's format.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage Guidelines

Use this command to define schemas for SLs interface bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple SLs schemas can be created to categorize SLs bulk statistics. All of the schemas are processed at each collection interval. To create multiple SLs schemas, re-issue the `sls schema schema_name` command using a different schema name each time.

Examples

Include the bulk statistic variable names to create an SLs schema named `stats_SLs_pkts_tx_rx` that specifies a collection of statistics (a schema format) for the total number of SCTP packets transmitted and received:

Use the following command:

```
sls schema stats_SLs_pkts_tx_rx format "Total SCTP Packets Sent: %sctp-totsent-pkts%
Total SCTP Packets Received: %sctp-totrec-pkts%n"
```
**ss7link schema**

Configures the collection of the SS7 link activity statistics.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

```
ss7link schema schema_name format schema_format
no ss7link schema schema_name
```

**no**

Removes the specified SS7 Link schema from statistics collection.

**schema_name**

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**format schema_format**

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the **Schema Format String Length**, on page 2013 section.

For information on the schema format's syntax, see the **Schema Format String Syntax**, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the **Statistics and Counters Reference**.
Usage Guidelines

Use this command to define schemas for SS7 link and linkset bulk statistics collection per SS7 routing domain in a generated stats report file. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple collection schemas can be created to categorize SS7 link bulk statistics. All of the schemas are processed at each collection interval. To create multiple SS7 link schemas, re-issue the `ss7link schema schema_name` command using a different schema name each time.

Examples

The following command creates a schema named `ss7lnk1stats1` that records the changeover orders sent and received per linkset and link and per SS7 routing domain:

```
ss7link schema ss7lnk1stats1 format "%ss7rd-number%-%ss7-linkset-id%-%ss7-link-id%-%ss7rd-asp_instance%-%ss7-link-mtp3-changeover-order-tx%-%ss7-link-mtp3-changeover-order-rx%"
```
ss7rd schema

Configures the collection of bulk statistics for SS7 routing domain services, which include the activity statistics for SCTP, MTP, and M3UA data.

**Important**

In Release 20.0, HNBGW is not supported. This command must not be used for HNBGW in Release 20.0. For more information, contact your Cisco account representative.

**Product**

SGSN
HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

`ss7rd schema schema_name format schema_format`

`no ss7rd schema schema_name`

no

Removes the specified SS7 routing domain schema from statistics collection.

`schema_name`

Specifies the schema's name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

`format schema_format`

Specifies the schema's format.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the [Schema Format String Length](#) on page 2013 section.

For information on the schema format's syntax, see [Schema Format String Syntax](#) on page 2013.
**Important**

For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage Guidelines**

Use this command to define schemas for collection of SS7 routing domain statistics to be included in the generated stats report file. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple collection schemas can be created to categorize SS7 routing domain bulk statistics. All of the schemas are processed at each collection interval. To create multiple SS7 routing domain schemas, re-issue the `ss7rd schema` command using a different schema name each time.

**Examples**

The following command creates a schema named `ss7rd1stats1` that identifies the SS7 routing domain and records the Application Server Process instance in the SS7 routing domain, along with the total number of sent and received SHUTDOWN messages per SS7 routing domain:

```plaintext
ss7rd schema ss7rd1stats1 format
"%%ss7rd-number%%-%%ss7rd-asp_instance%%-%%ss7rd-sctp-shutdown-tx%%-%%ss7rd-sctp-shutdown-rx%%"
```
tai schema

Configures TAI (Tracking Area Identifier) bulk statistics schema.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-bulkstats)#
```

**Syntax Description**

```
tai schema schema_name format schema_format
no tai schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema's name.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the format of the collected TAI statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages.
  `schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the [Schema Format String Length](#) on page 2013 section.
  For information on the schema format's syntax, see the [Schema Format String Syntax](#) on page 2013 section.

---

**Important**
For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.
**Usage Guidelines**

Use this command to define schemas for TAI bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified. Multiple TAI schemas can be created to categorize TAI bulk statistics. All of the schemas are processed at each collection interval. To create multiple TAI schemas, re-issue the `taischema schema_name` command using a different schema name each time.

**Important**

To enable collection of TAI schema bulk statistics, you must issue the MME Service Configuration Mode command: `statistics collection-mode tai`. Only those MME Services which are configured accordingly will provide TAI based statistics.

**Examples**

The following command creates a TAI schema with the following information: MNC, MCC, TAC, and the total number of paging attempts.

```
tai schema paging_attempted format "%tai-mnc% %tai-mcc% %tai-tac% %tai-paging-attempted%"
```
**transfer-interval**

Configures the frequency of transfer of collected statistics to the receiver.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax Description**

`transfer-interval minutes`

*minutes*

Specifies the number of minutes between the transfer of collected statistics to the receivers as an integer from 1 through 999999.

**Usage Guidelines**

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 (6 hours).

**Examples**

The following command sets the transfer interval to 24 hours (1440 minutes):

```
transfer-interval 1440
```
**vlan-npu schema**

Configures the collection of VLAN-NPU activity statistics.

---

**Important**
The VLAN-NPU counters will only be displayed if the `logical-port-statistics` command has been enabled at the interface level under the Ethernet Interface Configuration mode.

---

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```plaintext
[local] host_name(config-bulkstats)#
```

**Syntax Description**

```plaintext
vlan-npu schema  schema_name  [active-only] [format  schema_format]  
no  vlan-npu schema  schema_name
```

**no**
Removes the specified VLAN-NPU schema from statistics collection.

**schema_name**
Specifies the schema's name.

- `schema_name` must be an alphanumeric string of 1 through 31 characters.

**active-only**
Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

**format schema_format**
Specifies the schema's format.

- `schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the **Schema Format String Length**, on page 2013 section.

- For information on the schema format's syntax, see the **Schema Format String Syntax**, on page 2013 section.
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage Guidelines
Use this command to define schemas for VLAN-NPU bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple VLAN-NPU schemas can be created to categorize VLAN-NPU bulk statistics. All of the schemas are processed at each collection interval. To create multiple VLAN-NPU schemas, re-issue the `vlan-npu schema schema_name` command using a different schema name each time.

You can also use this command to restrict the VLAN-NPU schema statistics to those gathered on the Active ICSR chassis.

Examples
Include the bulk statistic variable names to create a VLAN-NPU schema named `vlanstats_vlan12` that specifies collection of statistics (a schema format) will be by VLAN-NPU interface for the total number of frames and bytes received with no Access Control List (ACL) match.

```
vlan-npu schema vlanstats_vlan12 format "VLAN12: %interfacename\nTotal Frames Recv'd with no ACL match: %no-acl-match-rx-frames\nTotal Bytes Recv'd with no ACL match: %no-acl-match-rx-bytes\n"
```
vrf schema

Configures VRF (Virtual Routing and Forwarding) bulk statistics schema.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax Description**

- `vrf schema schema_name [ active-only ] format schema_format`
- `no vrf schema schema_name`

`no`
Removes the specified schema.

`schema_name`
Specifies the schema's name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

`active-only`
Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

`format schema_format`
Specifies the schema's format.

`schema_format` must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**
For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
**Usage Guidelines**

Use this command to define schemas for VRF bulk statistics collection. Multiple LMA service schemas can be created to categorize VRF bulk statistics. All of the schemas are processed at each collection interval. To create multiple VRF schemas, re-issue the `vrf schema schema_name` command using a different schema name.

You can also use this command to restrict the VRF schema statistics to those gathered on the Active ICSR chassis.
wsg schema

Configures the collection of Wireless Security Gateway (WSG) activity statistics.

**Product**
WSG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local] <host_name>(config-bulkstats) #

**Syntax Description**

```
wsg schema  schema_name  [ active-only ] [ format  schema_format ]

no
wsg schema  schema_name
```

**no**

Removes the specified WSG schema from statistics collection.

**schema_name**

Specifies the schema's name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**active-only**

Specifies that the bulk statistics are to be gathered on the Active ICSR chassis only.

**format schema_format**

Specifies the schema's format.

*schema_format* must be a string of 1 through 3599 characters, including spaces within double quotation marks (" "). For more information, see the Schema Format String Length, on page 2013 section.

For information on the schema format's syntax, see the Schema Format String Syntax, on page 2013 section.

**Important**

For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

---

Command Line Interface Reference, Commands A - B, StarOS Release 20
Usage Guidelines

Use this command to define schemas for WSG bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple WSG schemas can be created to categorize WSG bulk statistics. All of the schemas are processed at each collection interval. To create multiple WSG schemas, re-issue the `wsg schema schema_name` command using a different schema name each time.

You can also use this command to restrict the WSG schema statistics to those gathered on the Active ICSR chassis.