Cisco ASR 5000 Series Command Line Interface Reference

Version 12.2

Last Updated April 30, 2012

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

Text Part Number: OL-25551-03

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

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

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

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

Cisco ASR 5000 Series Command Line Interface Reference

© 2012 Cisco Systems, Inc. and/or its affiliated entities. All rights reserved.

CONTENTS

About this Guide xcv
- Conventions Used xcvi
- Contacting Customer Support xcviii
- Additional Information xcix

Command Line Interface Overview 101
- CLI Structure 102
- CLI Command Modes 103
- CLI Administrative Users 104
  - Administrative User Types 104
  - Authenticating Administrative Users with RADIUS 104
    - RADIUS Mapping System 105
    - RADIUS Privileges 105
  - Administrative User Privileges 105
  - Allowed Commands per User Type 107
    - Inspector Mode Commands 107
    - Operator Mode Commands 108
    - Administrator Mode Commands 109
    - Security Administrator Mode Commands 109
- CLI Contexts 110
- Understanding the CLI Command Prompt 111
- CLI Command Syntax 112
- Entering and Viewing CLI Commands 113
  - Entering Partial CLI Commands 113
  - CLI Command Auto-completion 113
  - Using CLI Auto-Pagination 114
  - Using CLI Autoconfirmation 114
  - Regulating the Command Output 115
  - Viewing Command History 116
- Obtaining CLI Help 117
- Exiting the CLI and CLI Command Modes 118
  - Exiting Configuration Sub-modes 118
  - Exiting Global Configuration Mode 118
  - Ending a CLI Session 118
- Accessing the CLI 119
  - Accessing the CLI Locally Using the Console Port 119
  - Remotely Accessing the CLI 120
- IP Address Notation 121
  - IPv4 Dotted-Decimal Notation 121
  - IPv6 Colon-Separated Notation 121
  - CIDR Notation 121
- Alphanumeric Strings 123
  - Character Set 123
  - Quoted Strings 124

AAA Server Group Configuration Mode Commands 125

diameter accounting 126
diameter authentication 129
diameter authentication failure-handling 132
diameter dictionary 134
end 135
exit 136
radius 137
radius accounting 141
radius accounting apn-to-be-included 144
radius accounting algorithm 145
radius accounting billing-version 146
radius accounting gtp trigger-policy 147
radius accounting ha policy 148
radius accounting interim 149
radius accounting ip remote-address 150
radius accounting keepalive 151
radius accounting pdif trigger-policy 153
radius accounting rp 154
radius accounting server 157
radius algorithm 160
radius allow 161
radius attribute 162
radius authenticate 165
radius authenticator-validation 166
radius charging 167
radius charging accounting algorithm 169
radius charging accounting server 170
radius charging algorithm 172
radius charging server 173
radius ip vrf 175
radius keepalive 176
radius mediation-device 178
radius probe-interval 179
radius probe-max-retries 180
radius probe-timeout 181
radius server 182
radius trigger 185

AAL2 Node Configuration Mode Commands 187

aal2-path-id 188
end 190
exit 191
point-code 192

Accounting Policy Configuration Mode Commands 193

accounting-event-trigger 194
accounting-keys 196
accounting-level 197
accounting-mode 199
cc 200
end 203
exit 204
max-containers 205
operator-string 206

ACL Configuration Mode Commands 207

deny/permit (by source IP address masking) 208
deny/permit (any) 210
deny/permit (by host IP address) 212
deny/permit (by source ICMP packets) 214
deny/permit (by IP packets) 218
deny/permit (by TCP/UDP packets) 221
end 225
exit 226
readdress server 227
redirect context (by IP address masking) 231
redirect context (any) 233
redirect context (by host IP address) 235
redirect context (by source ICMP packets) 237
redirect context (by IP packets) 241
redirect context (by TCP/UDP packets) 244
redirect css delivery-sequence 248
redirect css service (any) 249
redirect css service (by host IP address) 251
redirect css service (by ICMP packets) 253
redirect css service (by IP packets) 256
redirect css service (by source IP address masking) 259
redirect css service (by TCP/UDP packets) 261
redirect css service (for downlink, any) 265
redirect css service (for downlink, by host IP address) 267
redirect css service (for downlink, by ICMP packets) 269
redirect css service (for downlink, by IP packets) 273
redirect css service (for downlink, by source IP address masking) 277
redirect css service (for downlink, by TCP/UDP packets) 279
redirect css service (for uplink, any) 284
redirect css service (for uplink, by host IP address) 286
redirect css service (for uplink, by ICMP packets) 288
redirect css service (for uplink, by IP packets) 292
redirect css service (for uplink, by source IP address masking) 295
redirect css service (for uplink, by TCP/UDP packets) 297
redirect nexthop (by IP address masking) 301
redirect nexthop (any) 304
redirect nexthop (by host IP address) 306
redirect nexthop (by source ICMP packets) 308
redirect nexthop (by IP packets) 312
redirect nexthop (by TCP/UDP packets) 316

ACS Bandwidth Policy Configuration Mode Commands 321

end 322
exit 323
flow limit-for-bandwidth 324
group-id 325

ACS Charging Action Configuration Mode Commands 327

allocation-retention-priority 328
billing-action 329
cca charging credit 332
charge-units 334
charge-volume 335

content-filtering processing server-group 338
content-id 339
end 340
exit 341
fair-usage 342
flow action 344
flow idle-timeout 349
flow limit-for-bandwidth 350
flow limit-for-flow-type 353
ip tos 354
ip vlan 356
nexthop-forwarding-address 357
qos-class-identifier 358
qos-renegotiate 359
retransmissions-counted 361
service-identifier 362
tft packet-filter 363
tos 364
tpo profile 366
video bitrate 367
video cae-readdressing 368
video detailed-statistics 369
video optimization-preprocessing all 370
video optimization-preprocessing cae-readdressing 371
video optimization-preprocessing transrating 372
video pacing by-policing 373
video transrating target-rate-reduction 375
xheader-insert 376

ACS Configuration Mode Commands 379

access-ruledef 380
bandwidth-policy 382
buffering-limit 383
charging-action 384
content-filtering category match-method 385
content-filtering category policy-id 386
credit-control 388
diameter credit-control 389
edr-format 390
edr-udr-flow-control 391
end 392
exit 393
fair-usage deact-margin 394
fair-usage tcp-proxy 395
fair-usage threshold-percent 396
firewall flow-recovery 397
firewall max-ip-packet-size 399
firewall mime-flood 400
firewall nat-alg 401
firewall no-ruledef-matches 403
firewall port-scan 404
firewall ruledef 406
firewall tcp-syn-flood-intercept 408
firewall track-list 409
fw-and-nat action 410

fw-and-nat policy 411
group-of-objects 412
group-of-prefixed-urls 414
group-of-ruledefs 415
h323 time-to-live 416
h323 timeout 417
h323 tpkt 419
h323 version 420
host-pool 421
idle-timeout 422
imsi-pool 424
ip dns-learnt-entries 425
ip max-fragments 426
label content-id 427
nat allocation-failure 428
nat allocation-in-progress 429
nat tcp-2msl-timeout 430
p2p-detection protocol 431
packet-filter 441
passive-mode 442
policy-control bearer-bw-limit 443
policy-control bind-default-bearer 444
policy-control burst-size 445
policy-control charging-action-override 446
policy-control charging-rule-base-name 447
policy-control dynamic-rule-limit 449
policy-control retransmissions-counted 450
policy-control update-default-bearer 451
port-map 452
redirect user-agent 453
rulebase 454
ruledef 455
system-limit l4-flows 456
tethering-database 457
timedef 459
tpo policy 460
tpo profile 461
udr-format 462
url-blacklisting match-method 463
xheader-format 464

ACS Group-of-Objects Configuration Mode Commands 465

end 466
exit 467
member-object 468

ACS Group-of-Prefixed-URLs Configuration Mode Commands 469

end 470
exit 471
prefixed-url 472

ACS Group-of-Ruledefs Configuration Mode Commands 473

add-ruledef 474
dynamic-command 475
end 476

exit 477
group-of-ruledefs-application 478
ACS Host Pool Configuration Mode Commands 481
end 482
exit 483
ip 484
ACS IMSI Pool Configuration Mode Commands 485
end 486
exit 487
imsi 488
ACS Packet Filter Configuration Mode Commands 489
direction 490
end 491
exit 492
ip local-port 493
ip protocol 494
ip remote-address 495
ip remote-port 496
priority 497
ACS Port Map Configuration Mode Commands 499
end 500
exit 501
port 502
ACS Rulebase Configuration Mode Commands 503
action priority 504
active-charging rf 507
bandwidth default-policy 509
billing-records 510
cca diameter requested-service-unit 512
cca quota 513
cca quota time-duration algorithm 515
cca radius accounting interval 517
cca radius charging context 518
cca radius user-password 519
charging-rule-optimization 520
constituent-policies 521
content-filtering category policy-id 523
content-filtering flow-any-error 524
content-filtering mode 525
dynamic-rule order 527
edr sn-charge-volume 528
edr suppress-zero-byte-records 529
edr transaction-complete 530
edr voip-call-end 532
egcdr inactivity-meter 534
egcdr cdr-encoding 535
egcdr tariff 536
egcdr threshold 537
egcdr time-duration algorithm 539
end 541
exit 542

extract-host-from-uri 543
fair-usage session-waiver-percent 544
firewall dos-protection 545
firewall flooding 548
firewall icmp-destination-unreachable-message-threshold 550
firewall max-ip-packet-size 551
firewall mime-flood 552
firewall no-ruledef-matches 553
firewall policy 555
firewall priority 556
firewall tcp-first-packet-non-syn 559
firewall tcp-idle-timeout-action 560
firewall tcp-reset-message-threshold 561
firewall tcp-syn-flood-intercept 562
flow any-error 564
flow control-handshaking 566
flow end-condition 568
flow limit-across-applications 571
fw-and-nat default-policy 573
ip reassembly-timeout 574
ip reset-tos 575
nat binding-record 576
nat policy 578
nat suppress-aaa-update call-termination 580
p2p dynamic-flow-detection 581
post-processing dynamic 582
post-processing policy 584
post-processing priority 586
qos-renegotiate timeout 588
radius threshold 589
route priority 590
rtp dynamic-flow-detection 593
ruledef-parsing 594
tcp 2msl-timeout 595
tcp check-window-size 596
tcp mss 597
tcp out-of-order-timeout 598
tcp packets-out-of-order 599
tcp proxy-mode 601
tethering-detection 603
timestamp rounding 604
tpo default-policy 606
transport-layer-checksum 607
udr threshold 608
udr trigger 610
url-blacklisting action 611
url-preprocessing 613
wtp out-of-order-timeout 614
wtp packets-out-of-order 615
xheader-encryption 617

ACS Ruledef Configuration Mode Commands 619

bearer 3gpp apn 620
bearer 3gpp imsi 621
bearer 3gpp rat-type 622

bearer 3gpp sgsn-address 623
bearer 3gpp2 bsid 624
bearer 3gpp2 service-option 626
bearer apn 627
bearer imsi 629
bearer rat-type 630
bearer sgsn-address 631
bearer traffic-group 632
cca quota-state 633
cca redirect-indicator 634
copy-packet-to-log 635
dns answer-name 636
dns any-match 638
dns previous-state 639
dns query-name 640
dns return-code 641
dns state 642
dns tid 643
email 644
end 646
exit 647
file-transfer any-match 648
file-transfer chunk-number 649
file-transfer current-chunk-length 650
file-transfer declared-chunk-length 651
file-transfer declared-file-size 652
file-transfer filename 653
file-transfer previous-state 654
file-transfer state 655
file-transfer transferred-file-size 657
ftp any-match 658
ftp client-ip-address 659
ftp client-port 660
ftp command args 661
ftp command id 662
ftp command name 663
ftp connection-type 665
ftp data-any-match 666
ftp filename 667
ftp pdu-length 668
ftp pdu-type 669
ftp previous-state 670
ftp reply code 671
ftp server-ip-address 672
ftp server-port 673
ftp session-length 674
ftp state 675
ftp url 676
ftp user 677
http any-match 678
http attribute-in-data 679
http attribute-in-url 680
http content disposition 681
http content length 682

http content type 683
http domain 684
http error 685
http first-request-packet 686
http header-length 687
http host 688
http payload-length 689
http pdu-length 690
http previous-state 691
http referer 692
http reply code 694
http request method 695
http session-length 696
http state 697
http transaction-length 698
http transfer-encoding 699
http uri 700
http url 701
http user-agent 703
http version 704
http x-header 705
icmp any-match 707
icmp code 708
icmp type 709
icmpv6 any-match 710
icmpv6 code 711
icmpv6 type 712
if-protocol 713
imap any-match 715
imap cc 716
imap command 717
imap content class 719
imap content type 720
imap date 721
imap final-reply 722
imap from 723
imap mail-size 724
imap mailbox-size 725
imap message-type 726
imap previous-state 727
imap session-length 728
imap session-previous-state 729
imap session-state 730
imap state 731
imap subject 732
imap to 733
ip any-match 734
ip downlink 735
ip dst-address 736
ip error 737
ip protocol 738
ip server-domain-name 740
ip server-ip-address 741
ip src-address 743

ip subscriber-ip-address 744
ip total-length 746
ip uplink 747
ip version 748
mms any-match 749
mms bcc 750
mms cc 751
mms content location 752
mms content type 753
mms downlink 754
mms from 755
mms message-id 756
mms pdu-type 757
mms previous-state 759
mms response status 761
mms state 762
mms status 764
mms subject 765
mms tid 766
mms to 767
mms uplink 768
mms version 769
multi-line-or all-lines 770
p2p any-match 771
p2p protocol 772
p2p traffic-type 777
pop3 any-match 778
pop3 command args 779
pop3 command id 780
pop3 command name 781
pop3 mail-size 782
pop3 pdu-length 783
pop3 pdu-type 784
pop3 previous-state 785
pop3 reply args 786
pop3 reply id 787
pop3 reply status 788
pop3 session-length 789
pop3 state 790
pop3 user-name 791
pptp any-match 792
pptp ctrl-msg-type 793
pptp gre any-match 794
rtcp any-match 795
rtcp jitter 796
rtcp parent-proto 797
rtcp pdu-length 798
rtcp rtsp-id 799
rtcp session-length 800
rtcp uri 801
rtp any-match 802
rtp parent-proto 803
rtp pdu-length 804
rtp rtsp-id 805

rtp session-length 806
rtp uri 807
rtsp any-match 808
rtsp content length 809
rtsp content type 810
rtsp date 811
rtsp previous-state 812
rtsp reply code 813
rtsp request method 814
rtsp request packet 815
rtsp rtp-seq 816
rtsp rtp-time 817
rtsp rtp-uri 818
rtsp session-id 819
rtsp session-length 820
rtsp state 821
rtsp uri 822
rtsp uri sub-part 823
rtsp user-agent 825
rule-application 826
sdp any-match 828
sdp connection-ip-address 829
sdp media-audio-port 830
sdp media-video-port 831
sdp uplink 832
secure-http any-match 833
secure-http uplink 834
sip any-match 835
sip call-id 836
sip content length 837
sip content type 838
sip from 839
sip previous-state 840
sip reply code 841
sip request method 842
sip request packet 843
sip state 844
sip to 845
sip uri 846
smtp any-match 848
smtp command arguments 849
smtp command id 850
smtp command name 851
smtp mail-size 852
smtp pdu-length 853
smtp previous-state 854
smtp recipient 855
smtp reply arguments 856
smtp reply id 857
smtp reply status 858
smtp sender 859
smtp session-length 860
smtp state 861
tcp analyzed out-of-order 862

tcp any-match 863
tcp connection-initiator 864
tcp downlink 865
tcp dst-port 866
tcp duplicate 868
tcp either-port 869
tcp error 871
tcp flag 872
tcp initial-handshake-lost 873
tcp payload 874
tcp payload-length 875
tcp previous-state 876
tcp proxy-prev-state 877
tcp proxy-state 879
tcp session-length 881
tcp src-port 882
tcp state 884
tcp uplink 885
tethering-detection 886
tftp any-match 887
tftp data-any-match 888
udp any-match 889
udp downlink 890
udp dst-port 891
udp either-port 893
udp payload starts-with 895
udp src-port 896
udp uplink 898
wsp any-match 899
wsp content type 900
wsp domain 901
wsp downlink 902
wsp first-request-packet 903
wsp host 904
wsp pdu-length 905
wsp pdu-type 906
wsp previous-state 908
wsp reply code 909
wsp session-length 910
wsp session-management 911
wsp state 913
wsp status 914
wsp tid 915
wsp total-length 916
wsp transfer-encoding 917
wsp uplink 918
wsp url 919
wsp user-agent 920
wsp x-header 921
wtp any-match 923
wtp downlink 924
wtp gtr 925
wtp pdu-length 926
wtp pdu-type 927

wtp previous-state 928
wtp rid 929
wtp state 930
wtp tid 931
wtp transaction class 932
wtp ttr 933
wtp uplink 934
www any-match 935
www content type 936
www domain 937
www downlink 938
www first-request-packet 939
www header-length 940
www host 941
www payload-length 942
www pdu-length 943
www previous-state 944
www reply code 945
www state 946
www transfer-encoding 947
www url 948

ACS Timedef Configuration Mode Commands 949

end 950
exit 951
start 952

ACS TPO Policy Configuration Mode Commands 955

ad-filter 956
end 957
exit 958
match-ad 959
match-rule no-ruledef-match 960
match-rule priority 961

ACS TPO Profile Configuration Mode Commands 963

end 964
exit 965
http 966
p2p-detected 969
tcp 970

ACS x-header Format Configuration Mode Commands 975

end 976
exit 977
insert 978

ALCAP Configuration Mode Commands 981

aal2-node 982
aal2-route 983
associate 985
end 986
exit 987
maximum reset-retransmission 988
self-point-code 989
timeout alcap 990

timeout stc 993
APN Configuration Mode Commands 995
aaa 996
access-link 998
accounting-mode 999
active-charging bandwidth-policy 1002
active-charging link-monitor tcp 1003
active-charging rulebase 1005
apn-ambr 1006
associate accounting-policy 1008
authentication 1009
bearer-control-mode 1013
cc-home 1015
cc-roaming 1017
cc-sgsn 1019
cc-visiting 1022
content-filtering category 1024
credit-control-group 1025
data-tunnel mtu 1026
data-tunneling ignore df-bit 1027
dcca origin endpoint 1028
dcca peer-select 1029
dhcp context-name 1030
dhcp lease-expiration-policy 1031
dhcp service-name 1032
dns 1033
ehrpd-access 1035
emergency-apn 1036
end 1037
exit 1038
firewall policy 1039
fw-and-nat policy 1040
gsm-qos negotiate 1041
gtpp group 1043
gtpp secondary-group 1045
idle-timeout-activity 1047
ims-auth-service 1048
ip access-group 1049
ip address alloc-method 1050
ip address pool 1053
ip context-name 1054
ip header-compression 1055
ip hide-service-address 1056
ip local-address 1057
ip multicast discard 1058
ip qos-dscp 1059
ip source-violation 1062
ip user-datagram-tos copy 1063
ipv6 access-group 1064
ipv6 dns 1065
ipv6 egress-address-filtering 1066
ipv6 initial-router-advt 1067
l3-to-l2-tunnel address-policy 1068
loadbalance-tunnel-peers 1069

long-duration-action detection 1070
long-duration-action disconnection 1071
max-contexts 1073
mbms bmsc-profile 1075
mbms bearer timeout 1076
mbms ue timeout 1077
mediation-device 1078
mobile-ip home-agent 1080
mobile-ip mn-aaa-removal-indication 1081
mobile-ip mn-ha-hash-algorithm 1082
mobile-ip mn-ha-shared-key 1083
mobile-ip mn-ha-spi 1084
mobile-ip required 1085
mobile-ip reverse-tunnel 1086
nai-construction 1087
nbns 1089
nexthop-forwarding-address 1090
npu qos 1091
outbound 1092
p-cscf 1093
pdp-type 1094
permission 1096
policy 1097
ppp 1098
proxy-mip 1100
qos negotiate-limit 1101
qos rate-limit 1103
qos-renegotiate 1106
qos traffic-police 1107
radius 1108
radius group 1109
radius returned-framed-ip-address 1110
radius returned-username 1111
restriction-value 1112
secondary ip pool 1114
selection-mode 1115
timeout 1116
timeout bearer-inactivity 1117
timeout emergency-inactivity 1118
timeout idle 1119
timeout long-duration 1120
tpo policy 1121
tunnel address-policy 1122
tunnel gre 1123
tunnel ipip 1124
tunnel ipsec 1125
tunnel l2tp 1126
virtual-apn 1129

APN Profile Configuration Mode 1133

address-resolution-mode 1134
apn-resolve-dns-query 1135
cc 1136
description 1138
direct-tunnel 1139

dns-extn 1140
end 1142
exit 1143
gateway-address 1144
gtp 1146
idle-mode-acl 1147
ip 1148
pdp-data-inactivity 1151
pdp-type-ipv4v6-override 1153
pgw-address 1154
qos apn-ambr 1155
qos class 1156
qos dedicated-bearer 1163
qos default-bearer 1164
qos prefer-as-cap 1165
qos rate-limit direction 1166
ranap allocation-retention-priority-ie 1170
restrict access-type 1173

APN Remap Table Configuration Mode 1175

apn-remap 1176
apn-selection-default 1178
blank-apn 1180
cc 1181
description 1183
end 1184
exit 1185
wildcard-apn 1186

ASN Gateway Service Configuration Mode Commands 1189

active-relay 1190
authentication 1191
bind 1192
bs-monitor 1193
end 1195
exit 1196
gre 1197
handover 1198
header-compression-rohc 1200
idle-mode 1202
local-data-tunnel 1203
max-retransmission 1204
mobile-access-gateway 1205
mobile-ip 1206
peer-asngw 1207
policy 1208
policy asngw-initiated-reauth 1210
policy overload 1212
ran-peer-map 1213
retransmission-timeout 1214
secondary-ip-hosts 1215
secondary-ip-hosts 1216
service-flow create-before-ip-alloc 1217

ASN Paging Controller Configuration Mode Commands 1219

asnpc-id 1220
bind 1221
end 1222
exit 1223
max-retransmission 1224
paging-announce 1225
paging-group 1226
peer-asngw 1227
peer-asnpc 1228
policy overload 1229
retransmission-timeout 1230
setup-timeout 1231
ASN Paging Group Configuration Mode Commands 1233
end 1234
exit 1235
paging 1236
ASN QoS Descriptor Configuration Mode Commands 1239
dscp 1240
end 1241
exit 1242
global-service-class-name 1243
schedule-type 1244
service-class-name 1247
ASN RAN Peer Map Configuration Mode Commands 1249
end 1250
exit 1251
ran-peer 1252
ASN Service Profile Configuration Mode Commands 1253
downlink-classifier 1254
downlink-qos-id 1255
end 1256
exit 1257
uplink-classifier 1258
uplink-qos-id 1259
ATM Port Configuration Mode Commands 1261
clock-source 1262
description 1263
end 1264
exit 1265
line-timing 1266
loopback 1267
preferred slot 1268
pvc 1269
shutdown 1271
snmp trap link-status 1272
threshold high-activity 1273
threshold monitoring 1275
threshold rx-utilization 1277
threshold tx-utilization 1279
toh-sdsf 1281
BFD Configuration Mode Commands 1283

bfd multihop-peer 1284
bfd nbr-group-name 1286
echo 1287
end 1288
exit 1289
slow-timers 1290
BGP Address-Family (IPv4/IPv6) Configuration Mode Commands 1291
end 1292
exit 1293
maximum-paths 1294
neighbor 1295
network 1299
redistribute 1300
BGP Address-Family (VPNv4) Configuration Mode Commands 1301
end 1302
exit 1303
neighbor 1304
BGP Address-Family (VRF) Configuration Mode Commands 1305
end 1306
exit 1307
neighbor 1308
redistribute 1311
BGP Configuration Mode Commands 1313
address-family ipv4 1314
address-family ipv6 1316
address-family vpnv4 1317
bgp 1318
distance 1319
end 1320
enforce-first-as 1321
exit 1322
ip vrf 1323
maximum-paths 1324
neighbor 1325
network 1329
redistribute 1330
router-id 1331
scan-time 1332
timers 1333
BGP IP VRF Configuration Mode Commands 1335
end 1336
exit 1337
route-distinguisher 1338
route-target 1339
BITS Port Configuration Mode Commands 1341
default 1342
description 1343
end 1344
exit 1345
mode 1346
preferred slot 1347

recover 1348
shutdown 1349
snmp trap link-status 1350
BMSC Profile Configuration Mode Commands 1351
end 1352
exit 1353
gmb diameter dictionary 1354
gmb diameter endpoint 1355
gmb diameter peer-select 1356
gmb user-data 1357
Bulk Statistics File Configuration Mode Commands 1359
Bulk Statistics Configuration Mode Commands 1361
Overview 1362
Schema Format String Syntax 1362
Common Statistics 1362
aal2 schema 1363
alcap schema 1364
apn schema 1365
asngw schema 1366
bcmcs schema 1367
card schema 1368
context schema 1370
cscf schema 1371
cs-network-ranap 1373
cs-network-rtp 1374
dcca schema 1375
default 1376
diameter-acct schema 1377
diameter-auth schema 1378
dlci-util schema 1379
dpca schema 1381
ecs schema 1382
egtpc schema 1383
end 1384
exit 1385
fa schema 1386
file 1387
fng schema 1388
footer 1389
gather-on-standby 1391
gprs schema 1392
gtpc schema 1394
gtpp schema 1395
gtpu schema 1396
ha schema 1397
header 1398
hnbgw-hnbap schema 1400
hnbgw-ranap schema 1402
hnbgw-rtp schema 1404
hnbgw-rua schema 1405
hnbgw-sctp schema 1406
hsgw schema 1407

imsa schema 1408
ippool schema 1409
ipsg schema 1410
lac schema 1411
limit 1413
lma schema 1414
lns schema 1415
local-directory 1416
mag schema 1417
mipv6ha schema 1418
mme schema 1419
mvs schema 1420
nat-realm schema 1421
pcc-af schema 1422
pcc-policy schema 1423
pcc-sp-endpt schema 1424
pcc-service schema 1425
pdif schema 1426
pgw schema 1427
port schema 1428
ppp schema 1429
ps-network-ranap 1430
radius schema 1431
receiver 1432
remotefile 1434
rp schema 1436
sample-interval 1437
sccp schema 1438
schema 1439
sgs schema 1440
sgsn schema 1441
sgtp schema 1442
sgw schema 1443
show variables 1444
ss7link schema 1447
ss7rd schema 1448
transfer-interval 1449

Call Control Profile Configuration Mode 1451

access-restriction-data 1452
accounting context 1454
accounting mode 1455
allocate-ptmsi-signature 1456
apn-restriction 1457
associate 1458
attach 1459
authenticate activate 1464
authenticate all-events 1466
authenticate attach 1468
authenticate detach 1470
authenticate on-first-vector 1471
authenticate rau 1472
authenticate service-request 1474
authenticate sms 1476
authenticate tau 1478

cc 1479
check-zone-code 1481
ciphering-algorithm-gprs 1482
csfb 1483
description 1484
diameter-result-code-mapping 1485
direct-tunnel 1486
dns-ggsn 1487
dns-sgsn 1488
dns-pgw 1489
dns-sgw 1490
encryption-algorithm-lte 1491
encryption-algorithm-umts 1492
end 1493
equivalent-plmn 1494
exit 1496
gmm information-in-messages 1497
gmm retrieve-equipment-identity 1499
gs-service 1501
gtp send 1502
gtpu fast-path 1504
gw-selection 1505
integrity-algorithm-lte 1506
integrity-algorithm-umts 1507
local-cause-code-mapping 1508
location-area-list 1509
lte-zone-code 1510
map 1512
map-service 1513
max-bearers-per-subscriber 1514
max-pdns-per-subscriber 1515
min-unused-auth-vectors 1516
network-feature-support-ie 1517
network-initiated-pdp-activation 1518
override-arp-with-ggsn-arp 1521
pdp-activate access-type 1522
pdp-activate allow 1523
pdp-activate restrict 1524
plmn-protocol 1525
ptmsi-reallocate 1526
ptmsi-signature-reallocate 1528
qos 1530
rau-inter 1532
rau-inter-plmn 1535
rau-intra 1538
re-authenticate 1541
regional-subscription-restriction 1542
reuse-authentication-triplets 1544
rfsp-override 1545
s1-reset 1546
sctp-down 1547
sgsn-address 1548
sgsn-core-nw-interface 1550
sgsn-number 1551

sgtp-service 1552
sms-mo 1553
sms-mt 1554
srns-inter 1555
srns-intra 1556
subscriber-control-inactivity 1557
super-charger 1559
tau 1560
treat-as-hplmn 1562
zone-code 1563

Call-Home Configuration Mode 1565

activate 1566
alert-group 1567
contact-email-addr 1569
contract-id 1570
customer-id 1571
end 1572
exit 1573
mail-server 1574
phone-number 1575
profile 1576
rate-limit 1577
sender 1578
site-id 1579
street-address 1580

Call-Home Profile Configuration Mode 1581

active 1582
destination 1583
end 1585
exit 1586
subscribe-to-alert-group 1587

CAMEL Service Configuration Mode Commands 1591

associate-sccp-network 1592
end 1593
exit 1594
tcap destination-address 1595
timeout 1596

Card Configuration Mode Commands 1599

aps 1600
end 1601
exit 1602
framing 1603
header-type 1605
initial-e1-framing 1606
link-aggregation 1607
mode 1608
redundancy 1610
redundant with 1612
service-type 1613
shutdown 1615

Channelized Port Configuration Mode Commands 1617

alarm-disable 1618
alarm-soak-timer 1619
clock-source 1620
description 1621
dlci 1622
end 1624
exit 1625
frame-relay 1626
hopath-sdsf 1628
line-timing 1629
loopback 1630
lopath-sdsf 1631
path 1632
preferred slot 1636
pwe3-cesopsn 1637
shutdown 1638
snmp trap link-status 1639
threshold high-activity 1640
threshold monitoring 1641
threshold rx-utilization 1643
threshold tx-utilization 1645
toh-sdsf 1647
vc-mapping 1648

Cipher Suite Configuration Mode Commands 1649

encryption 1650
end 1651
exit 1652
hmac 1653
key-exchange 1654

Class-Map Configuration Mode Commands 1655

end 1656
exit 1657
match any 1658
match dst-ip-address 1659
match dst-port-range 1660
match ip-tos 1661
match ipsec-spi 1662
match packet-size 1663
match protocol 1664
match src-ip-address 1666
match src-port-range 1667

Content Filtering Policy Configuration Mode Commands 1669

analyze 1670
discarded-flow-content-id 1674
end 1675
exit 1676
failure-action 1677
timeout action 1679

Content Filtering Server Group Configuration Mode Commands 1681

connection retry-timeout 1682
deny-message 1683
deny-response code 1684

dictionary 1685
end 1686
exit 1687
failure-action 1688
icap server 1691
origin address 1693
response-timeout 1694
timeout action 1695
url-extraction 1696

Context Configuration Mode Commands 1697

aaa accounting 1698
aaa authentication 1700
aaa constructed-nai 1702
aaa filter-id rulebase mapping 1704
aaa group 1705
aaa nai-policy 1706
access-list undefined 1707
administrator 1708
apn 1711
asn-qos-descriptor 1712
asn-service-profile 1714
asngw-service 1716
asnpc-service 1717
bfd-protocol 1718
bgp extended-asn-cap 1719
bmsc-profile 1720
busyout ip pool 1721
cae-group 1723
camel-service 1724
cipher-suite 1725
class-map 1726
closedrp-rp handoff 1727
config-administrator 1728
content-filtering 1731
credit-control-service 1732
crypto group 1733
crypto ipsec transform-set 1734
crypto map 1736
crypto template 1738
cscf access-profile 1739
cscf acl 1740
cscf diameter-selection 1741
cscf ifc-filter-criteria 1742
cscf ifc-spt-condition 1744
cscf ifc-spt-group 1746
cscf ifc-trigger-point 1748
cscf isc-template 1749
cscf last-route-profile 1750
cscf peer-servers 1752
cscf peer-servers-group 1754
cscf policy 1755
cscf prefix-table 1756
cscf routes 1757
cscf service 1758

cscf session-template 1760
cscf subdomain-routes 1761
cscf translation 1762
cscf urn-service-list 1763
css server 1764
dhcp-service 1765
diameter accounting 1767
diameter authentication 1770
diameter authentication failure-handling 1773
diameter dictionary 1775
diameter endpoint 1776
diameter sctp 1777
diameter origin 1778
dns-client 1779
domain 1780
eap-profile 1781
edr-module active-charging-service 1782
egtp-service 1783
end 1785
event-notif-endpoint 1786
exit 1787
external-inline-server 1788
fa-service 1789
firewall max-associations 1790
fng-service 1791
ggsn-service 1792
gprs-service 1793
gs-service 1794
gtpp algorithm 1795
gtpp attribute 1796
gtpp charging-agent 1802
gtpp data-request sequence-numbers 1803
gtpp dead-server suppress-cdrs 1804
gtpp deadtime 1805
gtpp detect-dead-server 1806
gtpp dictionary 1807
gtpp duplicate-hold-time 1809
gtpp echo-interval 1810
gtpp egcdr 1812
gtpp error-response 1815
gtpp group 1816
gtpp max-cdrs 1817
gtpp max-pdu-size 1818
gtpp max-retries 1819
gtpp node-id 1820
gtpp redirection-allowed 1821
gtpp redirection-disallowed 1822
gtpp server 1823
gtpp source-port-validation 1825
gtpp storage-server 1826
gtpp storage-server local file 1827
gtpp storage-server max-retries 1830
gtpp storage-server mode 1831
gtpp storage-server timeout 1832

gtpp suppress-cdrs zero-volume-and-duration 1833
gtpp timeout 1834
gtpp trigger 1835
gtpp transport-layer 1836
gtpu-service 1837
ha-service 1839
hnbgw-service 1840
hsgw-service 1842
hss-peer-service 1844
ikev1 disable-initial-contact 1846
ikev1 disable-phase1-rekey 1847
ikev1 keepalive dpd 1848
ikev1 policy 1850
ikev2-ikesa 1851
ims-auth-service 1852
ims-sh-service 1853
inspector 1854
interface 1856
ip access-group 1858
ip access-list 1859
ip arp 1860
ip as-path access-list 1861
ip dns-proxy source-address 1862
ip domain-lookup 1863
ip domain-name 1864
ip forward 1865
ip identification packet-size-threshold 1866
ip localhost 1867
ip name-servers 1868
ip pool 1869
ip prefix-list 1880
ip prefix-list sequence-number 1882
ip route 1883
ip routing maximum-paths 1886
ip routing overlap-pool 1887
ip vrf 1888
ipms 1890
ipsec 1891
ipsg-service 1892
ipv6 access-group 1894
ipv6 access-list 1895
ipv6 dns-proxy 1896
ipv6 neighbor 1897
ipv6 pool 1898
ipv6 route 1902
isakmp disable-phase1-rekey 1903
isakmp keepalive 1904
isakmp policy 1905
iups-service 1906
l2tp peer-dead-time 1907
lac-service 1908
lawful-intercept 1909
lawful-intercept dictionary 1910
lma-service 1911

lns-service 1913
logging 1914
mag-service 1916
map-service 1918
mme-service 1919
mobile-ip fa newcall 1921
mobile-ip ha assignment-table 1923
mobile-ip ha newcall 1924
mobile-ip ha reconnect 1926
mpls bgp forwarding 1927
mpls ip 1928
mseg-service 1929
nw-reachability server 1930
network-requested-pdp-context activate 1932
network-requested-pdp-context gsn-map 1934
network-requested-pdp-context hold-down-time 1935
network-requested-pdp-context interval 1936
network-requested-pdp-context sgsn-cache-time 1937
operator 1938
optimize pdsn inter-service-handoff 1940
pcc-af-service 1941
pcc-policy-service 1943
pcc-service 1945
pcc-sp-endpoint 1947
pdg-service 1949
pdif-service 1950
pdsn-service 1951
pgw-service 1952
pilot-packet 1954
policy 1955
policy-group 1956
policy-map 1957
ppp 1958
ppp magic-number 1963
ppp statistics 1964
proxy-dns intercept-list 1965
radius accounting 1967
radius accounting algorithm 1970
radius accounting apn-to-be-included 1971
radius accounting billing-version 1972
radius accounting gtp trigger-policy 1973
radius accounting ha policy 1974
radius accounting interim volume 1975
radius accounting ip remote-address 1976
radius accounting keepalive 1977
radius accounting rp 1979
radius accounting server 1982
radius algorithm 1985
radius allow 1986
radius attribute 1987
radius authenticate null-username 1989
radius authenticate apn-to-be-included 1990
radius authenticator-validation 1991
radius change-authorize-nas-ip 1992

radius charging 1995
radius charging accounting algorithm 1997
radius charging accounting server 1998
radius charging algorithm 2000
radius charging server 2001
radius deadtime 2003
radius detect-dead-server 2004
radius dictionary 2006
radius group 2008
radius ip vrf 2009
radius keepalive 2010
radius max-outstanding 2012
radius max-retries 2013
radius max-transmissions 2014
radius mediation-device 2015
radius probe-interval 2016
radius probe-max-retries 2017
radius probe-message 2018
radius probe-timeout 2019
radius server 2020
radius strip-domain 2023
radius timeout 2024
radius trigger 2025
route-access-list extended 2027
route-access-list named 2029
route-access-list standard 2030
route-map 2031
router 2033
server 2035
service-redundancy-protocol 2037
session-event-module 2038
sgsn-service 2039
sgs-service 2040
sgtp-service 2041
sgw-service 2042
ssh 2044
ssl 2045
subscriber 2046
threshold available-ip-pool-group 2048
threshold ha-service init-rrq-rcvd-rate 2050
threshold ip-pool-free 2051
threshold ip-pool-hold 2053
threshold ip-pool-release 2055
threshold ip-pool-used 2057
threshold monitoring 2059
threshold pdsn-service init-rrq-rcvd-rate 2061
udr-module active-charging-service 2062

Credit Control Configuration Mode Commands 2063

apn-name-to-be-included 2064
app-level-retransmission 2065
diameter dictionary 2066
diameter dynamic-rules request-quota 2067
diameter fui-redirected-flow 2068
diameter gsu-with-only-infinite-quota 2069

diameter ignore-returned-rulebase-id 2070
diameter ignore-service-id 2071
diameter mscc-final-unit-action terminate 2072
diameter mscc-per-ccr-update 2073
diameter origin host 2074
diameter origin endpoint 2075
diameter peer-select 2076
diameter pending-timeout 2079
diameter result-code 2080
diameter send-ccri 2082
diameter service-context-id 2083
diameter session failover 2084
diameter update-dictionary-avps 2085
end 2086
exit 2087
failure-handling 2088
mode 2091
pending-traffic-treatment 2092
quota 2094
quota request-trigger 2095
quota time-threshold 2096
quota units-threshold 2097
quota volume-threshold 2098
radius usage-reporting-algorithm 2099
redirect-indicator-received 2100
servers-unreachable 2101
timestamp-rounding 2106
trigger type 2107
usage-reporting 2109

Credit Control Service Configuration Mode Commands 2111

diameter dictionary 2112
diameter endpoint 2113
end 2114
exit 2115
failure-handling 2116
request timeout 2118

Crypto Group Configuration Mode Commands 2119

end 2120
exit 2121
match address 2122
match ip pool 2123
switchover 2124

Crypto Map Dynamic Configuration Mode Commands 2125

end 2126
exit 2127
set 2128

Crypto Map IKEv1 Configuration Mode Commands 2131

end 2132
exit 2133
match address 2134
match crypto group 2135
match ip pool 2136

set 2137
Crypto Map IKEv2-IPv6 Configuration Mode Commands 2141
authentication 2142
control-dont-fragment 2143
end 2144
exit 2145
ikev2-ikesa 2146
match 2147
payload 2148
peer 2149
Crypto Map IKEv2-IPv6 Payload Configuration Mode Commands 2151
end 2152
exit 2153
ipsec 2154
lifetime 2155
rekey 2156
Crypto Map Manual Configuration Mode Commands 2157
end 2158
exit 2159
match address 2160
set control-dont-fragment 2161
set peer 2162
set session-key 2163
set transform-set 2165
Crypto Template Configuration Mode Commands 2167
authentication 2168
ca-certificate list 2170
ca-crl list 2171
certificate 2172
control-dont-fragment 2173
default 2174
dns-handling 2176
dos cookie-challenge notify-payload 2178
end 2179
exit 2180
ikev2-ikesa 2181
keepalive 2183
max-childsa 2184
nai 2185
natt 2186
payload 2187
peer network 2188
Crypto Template IKEv2-Dynamic Payload Configuration Mode Commands 2189
default 2190
end 2191
exit 2192
ignore-rekeying-requests 2193
ip-address-allocation 2194
ipsec 2195
lifetime 2196
maximum-child-sa 2197

rekey 2198
tsi 2199
tsr 2200
Crypto Transform Set Configuration Mode Commands 2201
end 2202
exit 2203
mode 2204
CSCF Access Profile Configuration Mode Commands 2205
access-security-type 2206
authentication 2207
diameter-selection 2208
end 2209
exit 2210
pcrf-policy-control 2211
sigcomp 2212
timeout 2213
CSCF ACL Configuration Mode Commands 2215
after 2216
before 2217
deny 2218
end 2221
exit 2222
permit 2223
redirect 2226
CSCF AoR Policy Rules Configuration Mode Commands 2229
after 2230
aor 2231
before 2232
end 2233
exit 2234
CSCF Charging Configuration Mode Commands 2235
end 2236
exclude 2237
exit 2238
CSCF Crypto Template Configuration Mode Commands 2239
end 2240
exit 2241
ipsec 2242
CSCF Diameter Selection Configuration Mode Commands 2243
aaa-group 2244
end 2247
exit 2248
CSCF Emergency-CSCF Configuration Mode Commands 2249
end 2250
exit 2251
privacy 2252
psap-file 2253
CSCF Enforce Codec Policy Configuration Mode Commands 2255
dynamic-codec 2256

end 2258
exit 2259
static-codec 2260
CSCF IFC SPT Group Mode Commands 2263
end 2264
exit 2265
spt-condition 2266
CSCF IFC Trigger Point Mode Commands 2267
end 2268
exit 2269
spt-group 2270
CSCF ISC Template Configuration Mode Commands 2271
cnsa 2272
end 2274
exit 2275
filter-criteria 2276
CSCF Last Route Profile Criteria Configuration Mode Commands 2277
county-name 2278
end 2279
exit 2280
CSCF NPDB Client Configuration Mode Commands 2281
bind 2283
end 2285
exit 2286
npdb-primary-server 2287
npdb-secondary-server 2288
timeout 2289
CSCF PCRF-Policy-Control Configuration Mode Commands 2291
authorization mediatype 2292
authorization policy-interworking-failure 2293
end 2294
exit 2295
signaling-bearer-loss 2296
CSCF Peer Servers Configuration Mode Commands 2297
end 2298
exit 2299
hunting-method 2300
server 2301
CSCF Peer Servers Group Configuration Mode Commands 2303
end 2304
exit 2305
peer-servers 2306
CSCF Peer Server Monitoring Configuration Mode Commands 2307
dummy-as 2308
end 2309
exit 2310
ims-capable 2311
lro-selection-profile 2312
mode 2313

monitor-status 2314
nw-session-template 2316
registration 2317
tps-rate 2318
CSCF Policy Configuration Mode Commands 2319
aor-policy-rules 2320
end 2321
exit 2322
service-policy-rules 2323
CSCF Policy Rules Configuration Mode Commands 2325
allow-noauth 2326
allow-unsecure 2327
authorization 2328
end 2329
enforce-codec-policy 2330
exit 2331
max-cscf-concurrent-sessions 2332
policy 2333
qos 2334
video-sessions 2335
CSCF Prefix Table Configuration Mode Commands 2337
end 2338
exit 2339
number 2340
CSCF Proxy-CSCF Configuration Mode Commands 2341
allow rfc3261-ua-interworking 2342
core-reg-expiry-time 2343
diameter 2344
emergency 2348
emergency-call-mode 2349
end 2350
exit 2351
interrogating-cscf-role 2352
message-max-size 2353
network-id 2354
pcrf-policy-control 2355
peer-sbc 2356
plmn-id 2357
reg-preloaded-route 2358
reg-service-route 2359
reliable-prov-resp 2360
restoration-procedure 2361
security-parameters 2362
sigcomp 2363
sip-header 2364
sip-param 2365
store-session-path 2366
CSCF Routes Configuration Mode Commands 2367
after 2368
before 2369
end 2370

exit 2371
route 2372
CSCF Security Configuration Mode Commands 2381
auth-failure-weight 2382
bad-request-weight 2383
dos-prevention 2384
end 2385
exit 2386
forking-contact-limit 2387
greylist-duration 2388
per-aor-failure-limit 2389
per-ip-failure-limit 2390
threshold-rate 2391
CSCF Service Configuration Mode Commands 2393
RetryAfter-header-value 2394
access-service 2395
access-type 2396
allow-dereg 2398
bind 2399
caller-preference 2402
charging 2403
cnsa-media-profile 2404
core-service 2406
custom reg-binding 2407
custom response 2408
custom volte 2410
default-aor-domain 2411
emergency-cscf 2412
end 2413
exit 2414
history-info 2415
interface statistics sip 2416
interrogating-cscf 2417
ipv4-ipv6-interworking 2418
keepalive 2419
lawful-intercept 2421
li-packet-cable 2422
max-sipmsg-size 2423
media-bridging 2424
monitoring 2425
multiple-reg same-private-id 2426
nat-policy 2427
nat-pool 2429
policy 2430
policy-name 2433
proxy-cscf 2434
proxy-serving-cscf 2435
recurse-on-redirect-resp 2436
reject-on-cnsa-failure 2437
release-call-on-media-loss 2438
rfc3261-proxy 2439
serving-cscf 2440
serving-cscf-list 2441

session-timer 2442
strict-check configured-aor-domain 2443
strict-outbound 2444
subscriber-policy-override 2445
subscription 2446
support-content-type any 2448
tcp-proxy 2449
threshold 2450
timeout 2452
transport-switching 2455
trusted-domain-entity 2456

CSCF Serving-CSCF Configuration Mode Commands 2457

3gpp 2458
allow rfc3261-ua-interworking 2460
as-call invite-request-uri update 2461
authentication 2462
bgcf-proxy 2465
diversion-info 2466
end 2467
exit 2468
forking 2469
interrogating-cscf-role 2470
local-call-features 2471
network-id 2472
npdb-client 2473
policy 2474
registration lifetime 2475
reliable-prov-resp 2477
server-name 2478
sifc 2479
sip-header insert 2480
sip-request 2481
tas 2483
tas-service 2484
user-authorization 2485

CSCF Session Template Configuration Mode Commands 2487

end 2488
exit 2489
inbound-cscf-acl 2490
outbound-cscf-acl 2491
policy-profile 2492
route-list 2493
translation-list 2494
urn-service-list 2495

CSCF Signalling Compression Configuration Mode Commands 2497

compression-mode 2498
decompression-memory-size 2499
end 2500
exit 2501
state-memory-size 2502

CSCF SIP Proxy Configuration Mode Commands 2503

as-call 2504

authentication 2505
diversion-info 2507
emergency 2508
end 2509
exit 2510
registration 2511
reliable-prov-resp 2512
sifc 2513
sigcomp 2514
tas 2515
tas-service 2516
CSCF Subdomain-route List Configuration Mode Commands 2517
after 2518
before 2519
end 2520
exit 2521
route 2522
CSCF Translation Configuration Mode Commands 2523
after 2524
before 2525
end 2526
exit 2527
uri-readdress 2528
CSCF URI Readdress Configuration Mode Commands 2531
action 2532
end 2534
exit 2535
CSCF URN List Configuration Mode Commands 2537
cscf-urn-service-mapping 2538
end 2539
exit 2540
CSS Delivery Sequence Configuration Mode Commands 2541
end 2542
exit 2543
redirect service (any) 2544
CSS Service Configuration Mode Commands 2545
end 2546
exit 2547
recovery 2548
server-interface 2549
DHCP Service Configuration Mode Commands 2551
allow 2552
bind 2553
default 2555
dhcp chaddr-validate 2556
dhcp client-identifier 2557
dhcp deadtime 2558
dhcp detect-dead-server 2559
dhcp ip vrf 2560
dhcp server 2561

dhcp server selection-algorithm 2562
end 2563
exit 2564
lease-duration 2565
max-retransmissions 2566
retransmission-timeout 2567
T1-threshold 2568
T2-threshold 2569

Diameter Endpoint Configuration Mode Commands 2571

associate 2572
cea-timeout 2574
connection retry-timeout 2575
connection timeout 2576
destination-host-avp 2577
device-watchdog-request 2579
dpa-timeout 2580
dscp 2581
dynamic-peer-discovery 2582
dynamic-peer-failure-retry-count 2583
dynamic-peer-realm 2584
dynamic-route 2585
end 2586
exit 2587
load-balancing-algorithm 2588
max-outstanding 2589
origin address 2590
origin host 2591
origin realm 2593
peer 2594
response-timeout 2596
route-entry 2597
route-failure 2599
server-mode 2601
tls 2602
use-proxy 2604
vsa-support 2606
watchdog-timeout 2607

DLCI Configuration Mode Commands 2609

bind link 2610
end 2611
exit 2612
shaping 2613
shutdown 2614

DNS Client Configuration Mode Commands 2615

bind 2616
cache algorithm 2617
cache size 2618
cache ttl 2619
case-sensitive 2620
end 2621
exit 2622
resolver 2623

round-robin answers 2624
EAP Authentication Configuration Mode Commands 2625
eap-aka 2626
eap-gtc 2627
eap-md5 2628
end 2629
exit 2630
EAP Configuration Mode Commands 2631
end 2632
exit 2633
max-retry 2634
mode 2635
EAP Mode Configuration Mode Commands 2637
end 2638
exit 2639
method 2640
EDR Format Configuration Mode Commands 2641
attribute 2642
end 2650
event-label 2651
exit 2652
rule-variable 2653
EDR Module Configuration Mode Commands 2661
cdr 2662
end 2666
exit 2667
file 2668
eGTP Service Configuration Mode Commands 2673
associate 2674
end 2675
exit 2676
gtpc 2677
interface-type 2680
validation-mode 2681
Ethernet Interface Configuration Mode Commands 2683
crypto-map 2684
description 2685
end 2686
exit 2687
ip 2688
ip mtu 2690
ip ospf authentication-key 2691
ip ospf authentication-type 2692
ip ospf cost 2693
ip ospf intervals 2694
ip ospf message-digest-key 2695
ip ospf network 2696
ip ospf priority 2697
ipv6 access-group 2698
ipv6 address 2699

ipv6 ospf 2700
ipv6 router advertisement 2702
policy-forward 2703
pool-share-protocol 2704
port-switch-on-L3-fail 2706
vlan-map 2708

Ethernet Port Configuration Mode Commands 2709

bind interface 2710
default 2711
description 2712
end 2713
exit 2714
fault-unidirect-mode 2715
flow-control 2716
ingress-mode 2717
link-aggregation 2718
media 2721
medium 2722
preferred slot 2723
shutdown 2724
snmp trap link-status 2725
srp virtual-mac-address 2726
threshold high-activity 2727
threshold monitoring 2728
threshold rx-utilization 2730
threshold tx-utilization 2732
vlan 2734

Exec Mode Commands (A-C) 2737

aaa test 2738
active-charging service 2739
alarm 2740
aps 2741
autoconfirm 2742
bulkstats force 2743
call-home send 2744
call-home test 2745
card busy-out 2746
card halt 2748
card migrate 2749
card reboot 2750
card restart 2752
card switch 2754
card upgrade 2755
cdr-push 2756
chassis 2757
clear aaa 2758
clear active-charging analyzer statistics 2759
clear active-charging charging-action statistics 2764
clear active-charging content-filtering server-group statistics 2765
clear active-charging credit-control statistics 2766
clear active-charging dns-learnt-ip-addresses 2767
clear active-charging edr-format statistics 2768
clear active-charging edr-udr-file statistics 2769

clear active-charging firewall statistics 2770
clear active-charging firewall track-list 2772
clear active-charging fw-and-nat policy statistics 2773
clear active-charging group-of-ruledefs statistics 2774
clear active-charging nat statistics 2775
clear active-charging rulebase statistics 2776
clear active-charging ruledef statistics 2777
clear active-charging subsystem 2778
clear active-charging tcp-proxy statistics 2779
clear active-charging tethering-detection statistics 2780
clear active-charging tpo policy statistics 2781
clear active-charging tpo profile statistics 2782
clear active-charging url-blacklisting statistics 2783
clear active-charging video detailed-statistics 2784
clear administrator 2785
clear alarm 2786
clear alcap 2787
clear asngw-service 2788
clear asnpc-service 2789
clear apn statistics 2790
clear bcmcs statistics 2791
clear blacklisted-gtpu-bind-address 2792
clear bssap+ statistics 2793
clear bssgp statistics 2794
clear bulkstats 2795
clear cae-group statistics server 2796
clear config 2797
clear congestion-control statistics 2798
clear content-filtering category statistics 2800
clear crash 2801
clear credit-control statistics 2802
clear crypto 2803
clear cs-network statistics 2805
clear cscf service 2806
clear cscf sessions 2808
clear cscf sip 2809
clear cscf subscription 2810
clear diameter-service 2811
clear diameter aaa-statistics 2813
clear diameter statistics 2814
clear dhcp statistics 2815
clear dns-client 2816
clear egtpc 2817
clear event-notif statistics 2819
clear firewall 2820
clear fng-service statistics 2821
clear gmm-sm statistics 2822
clear gprsns statistics 2825
clear gprsssf statistics 2826
clear gtpc statistics 2827
clear gtpp statistics 2829
clear gtpp storage-server local file statistics 2830
clear gtpp storage-server statistics 2831
clear gtpu statistics 2832

clear hd-storage-policy 2833
clear hnbgw sessions 2834
clear hnbgw statistics 2836
clear hsgw-service 2838
clear hss-peer-service 2839
clear ims-authorization 2840
clear ip access-group statistics 2841
clear ip arp 2842
clear ip bgp peer 2843
clear ip localhosts 2844
clear ip ospf process 2845
clear ipv6 neighbors 2846
clear ipv6 ospf process 2847
clear l2tp 2848
clear lawful-intercept 2850
clear llc statistics 2851
clear lma-service statistics 2852
clear local-policy 2853
clear local-user 2854
clear mag-service statistics 2855
clear maximum-temperatures 2856
clear mipfa statistics 2857
clear mipha statistics 2858
clear mme-service db record 2859
clear mme-service db statistics 2860
clear mme-service statistics 2861
clear multicast-sessions 2862
clear orbem statistics 2864
clear pcc-policy service statistics 2865
clear pcc-policy session 2866
clear pcc-sp-endpoint statistics 2868
clear pdg-service statistics 2869
clear pgw-service 2870
clear port 2871
clear ppp statistics 2872
clear prepaid 3gpp2 statistics 2873
clear prepaid wimax 2874
clear ps-network statistics 2875
clear qos npu stats 2876
clear radius accounting archive 2877
clear radius counters 2878
clear rohc statistics 2879
clear rp service-option 2880
clear rp statistics 2881
clear sccp statistics 2882
clear session disconnect-reasons 2884
clear session-event-record statistics 2885
clear session setuptime 2886
clear session subsystem 2887
clear sgsn-fast-path statistics 2888
clear sgsn-map-app 2889
clear sgs-service 2890
clear sgtpc statistics 2891
clear sgtpu statistics 2892

clear sgw-service statistics 2894
clear sms statistics 2895
clear sndcp statistics 2896
clear snmp trap 2897
clear srp 2898
clear ssl statistics 2899
clear subscribers 2900
clear super-charger 2912
clear tcap statistics 2913
cli 2914
clock set 2915
configure 2916
context 2918
copy 2919
crash copy 2921
crypto-group 2923

Exec Mode Commands (D-S) 2925

debug 2926
debug bfd 2927
debug ip 2928
debug ip bgp 2929
debug ip ospf all 2931
debug ip ospf event 2932
debug ip ospf ism 2933
debug ip ospf lsa 2934
debug ip ospf nsm 2935
debug ip ospf packet 2936
debug ip ospf route 2938
debug ip ospf router 2939
debug ipv6 ospf all 2940
debug ipv6 ospf event 2941
debug ipv6 ospf ifsm 2942
debug ipv6 ospf lsa 2943
debug ipv6 ospf nsm 2944
debug ipv6 ospf packet 2945
debug ipv6 ospf route 2947
default terminal 2948
delete 2949
dhcp force 2950
dhcp test 2951
diameter disable endpoint 2952
diameter enable endpoint 2953
diameter reset connection 2954
diameter reset route failure 2955
directory 2956
disable radius 2957
dns-client 2958
enable radius 2959
exit 2960
filesystem 2961
filesystem synchronize 2962
gtpc test echo 2963
gtpp interim now 2964
gtpp interim now active-charging egcdr 2967

gtpp storage-server commit 2968
gtpp test 2969
gtpu test echo 2970
gtpv0 test echo 2971
hd raid 2972
host 2974
interface 2975
lawful-intercept 2976
lawful-intercept packet-cable 2977
lawful-intercept ssdf 2978
link-aggregation port switch to 2979
logging active 2980
logging filter 2982
logging trace 2990
logs checkpoint 2992
lsp-ping 2993
lsp-traceroute 2994
mkdir 2995
mme offload 2996
mme reset 2997
monitor protocol 2998
monitor subscriber 3001
newcall policy 3005
password change 3009
ping 3010
ping6 3012
port switch to 3014
ppp echo-test 3015
radius interim accounting now 3017
radius test 3018
reload 3020
rename 3021
reveal disabled commands 3023
rlogin 3024
rmdir 3025
rotate-hd-file 3026
save configuration 3027
save logs 3029
session trace 3038
setup 3041
sgs offload 3042
sgsn clear-detached-subscriptions 3044
sgsn imsimgr 3045
sgsn offload 3046
sgsn op 3048
sgsn retry-unavailable-ggsn 3052
sgtpc test echo sgsn-address 3053
shutdown 3054
sleep 3055
srp initiate-switchover 3056
srp reset-auth-probe-fail 3057
srp reset-diameter-fail 3058
srp terminate-post-process 3059
srp validate-configuration 3060

srp validate-switchover 3061
ssh 3062
start crypto security-association 3063
system 3064
Exec Mode (T-Z) 3067
telnet 3068
terminal 3069
test alarm 3070
test ipcf bindmux 3071
test ipsec tunnel 3072
test mobile tunnel 3073
timestamps 3074
traceroute 3075
update active-charging 3077
update cscf 3079
update firewall policy 3081
update ip 3082
update qos policy map 3083
update qos tft 3085
upgrade 3086
upgrade content-filtering 3088
upgrade tethering-detection 3089
upgrade url-blacklisting database 3090
Exec Mode Show Commands (A-C) 3091
show aaa 3092
show active-charging analyzer statistics 3093
show active-charging bandwidth-policy 3095
show active-charging charging-action 3096
show active-charging content-filtering category policy-id 3097
show active-charging content-filtering category statistics 3098
show active-charging content-filtering server-group 3099
show active-charging credit-control 3101
show active-charging dns-learnt-ip-addresses 3102
show active-charging edr-format 3104
show active-charging edr-udr-file 3105
show active-charging file-space-usage 3106
show active-charging firewall statistics 3107
show active-charging firewall track-list 3109
show active-charging flows 3110
show active-charging flow-mappings 3118
show active-charging fw-and-nat policy 3119
show active-charging group-of-prefixed-urls 3120
show active-charging group-of-ruledefs 3121
show active-charging nat statistics 3122
show active-charging packet-filter 3123
show active-charging rulebase 3124
show active-charging ruledef 3125
show active-charging service 3127
show active-charging sessions 3128
show active-charging subsystem 3135
show active-charging tcp-proxy statistics 3136
show active-charging tethering-detection 3138
show active-charging timedef 3140

show active-charging tpo policy statistics 3141
show active-charging tpo profile statistics 3142
show active-charging udr-format 3143
show active-charging url-blacklisting statistics 3144
show active-charging video detailed-statistics 3145
show active-charging xheader-format 3146
show administrators 3147
show alarm 3148
show alcap counters 3150
show alcap-service 3151
show alcap statistics 3152
show apn 3153
show apn counters ip-allocation 3154
show apn statistics 3155
show apn-profile 3156
show aps 3157
show apn-remap-table 3159
show asngw-service 3160
show asngw-service session 3162
show asngw-service session counters 3164
show asngw-service statistics 3166
show asnpc-service 3168
show asnpc-service session 3169
show asnpc-service session counters 3171
show asnpc-service session counters verbose 3172
show asnpc-service statistics 3174
show asnpc-service statistics verbose 3175
show banner 3176
show bcmcs counters 3177
show bcmcs statistics 3178
show boot 3179
show bssap+ statistics 3180
show bssgp statistics 3181
show bssgp status 3183
show bulkstats 3184
show ca-certificate 3188
show ca-crl 3189
show cae-group server 3190
show call-control-profile 3191
show call-home 3192
show call-control-profile 3194
show camel-service 3195
show certificate 3196
show cli 3197
show clock 3198
show configuration 3199
show configuration errors 3203
show congestion-control 3207
show content-filtering category database 3209
show content-filtering category policy-id 3211
show content-filtering category statistics 3212
show content-filtering category url 3214
show content-filtering server-group 3215
show context 3216

show cpu 3217
show crash 3219
show credit-control sessions 3220
show credit-control statistics 3221
show crypto group 3222
show crypto ikev1 3223
show crypto ikev2-ikesa security-associations summary 3224
show crypto ikev2-ikesa transform-set 3225
show crypto ipsec 3226
show crypto ipsec transform-set 3228
show crypto isakmp keys 3229
show crypto isakmp policy 3230
show crypto isakmp security-associations 3231
show crypto managers 3232
show crypto map 3233
show crypto statistics 3234
show crypto transform-set 3235
show cs-network 3236
show cs-network counters 3237
show cs-network statistics 3238
show cscf ifc 3240
show cscf nat 3241
show cscf npdb-servers 3242
show cscf peer-servers 3243
show cscf service 3244
show cscf sessions 3247
show cscf sip 3249
show cscf tcp 3251
show css delivery-sequence 3253
show css server 3254
show css service 3255

Exec Mode Show Commands (D-G) 3257

show dhcp 3258
show dhcp statistics 3260
show dhcp-service 3261
show dhcp status 3262
show diameter aaa-statistics 3263
show diameter accounting servers aaa-group 3264
show diameter authentication servers aaa-group 3265
show diameter endpoint 3266
show diameter endpoints 3267
show diameter message-queue 3268
show diameter peers 3270
show diameter route status 3272
show diameter route table 3274
show diameter statistics 3275
show diameter-service 3276
show dns-client 3277
show dynamic-policy statistics 3278
show egtpc peers 3279
show egtpc sessions 3281
show egtpc statistics 3283
show egtp-service 3285
show event-notif server 3286

show event-notif statistics 3287
show external-inline-servers 3288
show fa-service 3289
show fans 3290
show file 3291
show firewall flows 3293
show firewall ruledef 3294
show firewall statistics 3295
show fng-service 3296
show fng-service session 3298
show fng-service statistics 3300
show freeze-ptmsi imsi 3301
show ggsn-service 3302
show ggsn-service sgsn-table 3303
show global-title-translation 3304
show gmm-sm statistics 3305
show gprsns statistics 3308
show gprsns status 3309
show gprs-service 3310
show gprsssf 3311
show gs-service 3313
show gtpc 3314
show gtpc statistics 3316
show gtpp 3318
show gtpp accounting 3319
show gtpp counters 3320
show gtpp group 3321
show gtpp statistics 3322
show gtpp storage-server 3323
show gtpu statistics 3325
show gtpu-service 3326

Exec Mode Show Commands (H-L) 3327

show ha-service 3328
show hardware 3329
show hd raid 3331
show hd-storage-policy 3332
show hnbgw access-control-db 3333
show hnbgw counters 3334
show hnbgw sessions 3335
show hnbgw statistics hnbgw-service 3338
show hnbgw statistics hnbid 3340
show hnbgw-service 3342
show hsgw-service 3343
show hss-peer-service 3345
show imei-profile 3347
show ims-authorization policy-control 3348
show ims-authorization policy-gate 3349
show ims-authorization servers 3351
show ims-authorization service 3352
show ims-authorization sessions 3354
show ip 3356
show ip as-path-access-list 3358
show ip bgp 3359
show ip interface 3361

show ip ospf 3363
show ip policy-forward 3365
show ip pool 3366
show ip ipsp 3369
show ip traffic sctp 3370
show ipms status 3371
show ipsg 3372
show ipv6 3374
show ipv6 ospf 3376
show ipv6 pool 3378
show ipv6 prefix-list 3379
show ipv6 route 3381
show ipv6 route-access-list 3382
show iups-service 3383
show l2tp sessions 3385
show l2tp statistics 3387
show l2tp tunnels 3388
show lawful-intercept 3390
show lawful-intercept ssdf statistics 3391
show lac-service 3392
show leds 3393
show license information 3394
show linecard 3395
show linkmgr 3397
show llc statistics 3398
show llc status 3399
show lma-service 3401
show lns-service 3403
show local-user 3404
show logging 3406
show logs 3407
show lte-policy 3416

Exec Mode Show Commands (M-P) 3419

show mag-service 3420
show map-service 3422
show map statistics 3423
show maximum-temperatures 3424
show mbms bearer-service 3425
show mipfa 3427
show mipha 3430
show mipv6ha 3433
show mme-service 3435
show mme-service db record 3436
show mme-service db statistics 3438
show mme-service enodeb-association 3439
show mme-service session 3441
show mme-service statistics 3444
show mpls ldp 3446
show mseg-config 3448
show mseg-service 3449
show multicast-sessions 3450
show network-requested-pdp-context 3453
show network-service-entity 3454
show npu error-counters 3455

show npu utilization 3456
show ntp 3457
show nw-reachability server 3458
show operator-policy 3459
show orbem 3460
show patch-progress 3462
show pcc-af service 3463
show pcc-af session 3464
show pcc-policy service 3466
show pcc-policy session 3467
show pcc-service 3469
show pcc-service session 3470
show pcc-service statistics 3472
show pcc-sp-endpoint 3473
show pcc-sp-endpoint connection 3474
show pdg-service 3475
show pdg-service statistics 3476
show pdif-service 3477
show pdsn-service 3478
show pgw-service 3479
show port 3480
show power 3482
show ppp 3483
show prepaid 3gpp2 3485
show prepaid wimax 3487
show profile-id-qci-mapping 3489

Exec Mode Show Commands (Q-S) 3491

show qci-qos-mapping 3492
show qos npu inter-subscriber traffic 3493
show radius 3494
show radius charging servers 3496
show radius client 3497
show radius counters 3498
show resources 3500
show rohc counters 3501
show rohc statistics 3503
show route-map 3504
show rp 3505
show rp service-option 3507
show rp statistics 3508
show rsvp counters 3510
show rsvp statistics 3511
show sccp-network 3512
show sccp statistics 3513
show sctp-param-template 3515
show session counters historical 3516
show session counters pcf-summary 3519
show session disconnect-reasons 3520
show session duration 3521
show session-event-record 3523
show session progress 3524
show session recovery status 3527
show session setuptime 3528
show session subsystem 3529

show session trace 3531
show sgs-service 3533
show sgsn-operator-policy 3534
show sgsn 3535
show sgsn-fast-path 3536
show sgsn-map-app 3537
show sgsn-mode 3538
show sgsn-pool 3539
show sgsn-service 3540
show sgtp-service 3541
show sgtpc statistics 3543
show sgtpu statistics 3544
show sgw-service 3546
show sms statistics 3547
show sndcp statistics 3548
show snmp 3549
show srp 3551
show ss7-routing-domain 3553
show ssh key 3556
show ssl cipher-suite 3557
show ssl connection 3558
show ssl map 3559
show ssl statistics 3560
show subscribers 3561
show super-charger 3581
show support details 3582
show system uptime 3584

Exec Mode Show Commands (T-Z) 3585

show tacacs 3586
show task 3587
show tcap statistics 3591
show temperature 3592
show terminal 3593
show threshold 3594
show timing 3595
show upgrade 3596
show url-blacklisting database 3597
show version 3599

FA Service Configuration Mode Commands 3601

advertise 3602
authentication aaa 3604
authentication mn-aaa 3605
authentication mn-ha 3607
bind 3608
challenge-window 3610
default subscriber 3611
dynamic-ha-assignment 3612
dynamic-mip-key-update 3613
encapsulation allow gre 3614
end 3615
exit 3616
fa-ha-spi 3617
gre 3620

ha-monitor 3622
idle-timeout-mode 3624
ignore-mip-key-data 3625
ignore-stale-challenge 3626
ip local-port 3627
isakmp 3628
limit-reg-lifetime 3630
max-challenge-len 3631
mn-aaa-removal-indication 3632
multiple-reg 3633
optimize tunnel-reassembly 3634
private-address allow-no-reverse-tunnel 3635
proxy-mip 3636
reg-timeout 3638
reverse-tunnel 3639
revocation 3640
threshold reg-reply-error 3642

Firewall-and-NAT Action Configuration Mode Commands 3645

end 3646
exit 3647
flow check-point 3648

Firewall-and-NAT Policy Configuration Mode Commands 3649

access-rule 3650
end 3654
exit 3655
firewall dos-protection 3656
firewall flooding 3660
firewall icmp-checksum-error 3662
firewall icmp-destination-unreachable-message-threshold 3663
firewall icmp-echo-id-zero 3664
firewall icmp-fsm 3665
firewall ip-reassembly-failure 3666
firewall malformed-packets 3667
firewall max-ip-packet-size 3668
firewall mime-flood 3669
firewall policy 3671
firewall tcp-checksum-error 3673
firewall tcp-first-packet-non-syn 3674
firewall tcp-fsm 3675
firewall tcp-idle-timeout-action 3676
firewall tcp-options-error 3677
firewall tcp-partial-connection-timeout 3678
firewall tcp-reset-message-threshold 3679
firewall tcp-syn-flood-intercept 3680
firewall tcp-syn-with-ecn-cwr 3682
firewall udp-checksum-error 3683
firewall validate-ip-options 3684
nat binding-record 3685
nat icsr-flow-recovery 3686
nat policy 3687
nat private-ip-flow-timeout 3689
nat suppress-aaa-update 3690

Firewall-and-NAT Access Ruledef Configuration Mode Commands 3691
bearer 3gpp apn 3692
bearer 3gpp imsi 3693
bearer username 3694
create-log-record 3695
end 3696
exit 3697
icmp any-match 3698
icmp code 3699
icmp type 3700
icmpv6 any-match 3701
icmpv6 code 3702
icmpv6 type 3703
ip any-match 3704
ip downlink 3705
ip dst-address 3706
ip protocol 3707
ip server-ipv6-network-prefix 3709
ip src-address 3710
ip uplink 3711
ip version 3712
tcp any-match 3713
tcp dst-port 3714
tcp either-port 3716
tcp src-port 3718
udp any-match 3720
udp dst-port 3721
udp either-port 3723
udp src-port 3725

FNG Service Configuration Mode Commands 3727
aaa aggregation 3728
aaa authentication 3730
bind 3731
default 3732
duplicate-session-detection 3733
ip source-violation 3734
setup-timeout 3735

FTP Configuration Mode Commands 3737
end 3738
exit 3739
max servers 3740
timeout 3741

GGSN Service Configuration Mode Commands 3743
accounting 3744
associate gtpu-service 3745
associate pgw-service 3746
authorize-with-hss 3747
bind 3748
cc behavior 3750
cc profile 3751
default 3754
dns-client 3756

echo-interval 3757
end 3759
exit 3760
fqdn 3761
gtpc nsapi-in-create-pdp-response 3763
gtpc private-extension 3764
gtpc ran-procedure-ready-delay 3766
gtpu echo-interval 3768
guard-interval 3769
ip local-port 3770
ip qos-dscp 3771
max-retransmissions 3774
mbms policy 3775
newcall 3776
path-failure 3777
plmn id 3778
plmn unlisted-sgsn 3779
policy 3781
retransmission-timeout 3782
setup-timeout 3783
sgsn address 3784
sgsn define-multiple-address-group 3786
sgsn multiple-address-group 3787
sgsn mcc-mnc 3789
trace-collection-entity 3790

Global Configuration Mode Commands 3791

aaa accounting-overload-protection 3792
aaa default-domain 3793
aaa domain-matching ignore-case 3794
aaa domain-matching imsi-prefix 3795
aaa large-configuration 3796
aaa last-resort 3797
aaa tacacs+ 3798
aaa username-format 3799
active-charging service 3800
alarm 3801
apn-profile 3802
apn-remap-table 3803
arp 3804
autoconfirm 3805
autoless 3806
banner 3807
boot delay 3809
boot interface 3810
boot nameserver 3812
boot system priority 3813
bulkstats 3816
ca-certificate 3818
ca-crl 3820
card 3822
card-standby-priority 3823
call-control-profile 3824
cdr-multi-mode 3825
certificate 3826

cli 3828
clock 3830
congestion-control 3833
congestion-control overload-disconnect 3834
congestion-control policy 3836
congestion-control threshold 3840
content-filtering category database directory 3844
content-filtering category database max-versions 3845
content-filtering category database override 3846
context 3847
crash enable 3848
cs-network 3850
css acsmgr-selection-attempts 3852
css delivery-sequence 3853
css service 3854
default 3855
diameter-proxy ram-disk 3859
ecmp-lag hash 3860
end 3861
enforce imsi-min equivalence 3862
exit 3863
fa-spi-list 3864
global-title-translation address-map 3865
global-title-translation association 3866
gtpp compression-process 3867
gtpp ram-disk-limit 3868
gtpp single-source 3869
ha-spi-list 3871
hd raid 3872
hd storage-policy 3873
high-availability 3874
hybrid-mode 3875
imei-profile 3876
license 3877
line 3878
link-aggregation 3879
local-policy-service 3880
local-user allow-aaa-authentication 3882
local-user lockout-time 3883
local-user max-failed-logins 3884
local-user password 3885
local-user username 3888
logging console 3891
logging disable 3892
logging display 3893
logging filter 3894
logging monitor 3901
logging runtime 3902
lte-policy 3903
mediation-device 3904
mobile-services-edge-gateway 3905
network-overload-protection 3906
network-service-entity 3908
network-service-entity ip 3909

ntp 3910
operator-policy 3911
orbem 3913
pac-standby-priority 3914
port atm 3915
port bits 3916
port channelized 3917
port ethernet 3918
port mac-address virtual-base-address 3919
port rs232 3920
profile-id-qci-mapping 3921
ps-network 3922
qci-qos-mapping 3924
qos npu inter-subscriber traffic bandwidth 3925
qos npu inter-subscriber traffic bandwidth-sharing 3927
qos npu inter-subscriber traffic priority 3929
ran-peer-map 3931
require active-charging 3932
require cipher ssl resource-percentage 3934
require demux card 3935
require detailed-rohc-stats 3936
require diameter-proxy 3937
require ecs credit-control subscriber-mode 3938
require session recovery 3939
reveal disabled commands 3940
rohc-profile 3941
sccp-network 3943
sctp-parameter-template 3944
session trace 3945
sgsn-global 3947
snmp authentication-failure-trap 3948
snmp community 3949
snmp engine-id 3951
snmp heartbeat 3952
snmp history heartbeat 3953
snmp notif-threshold 3954
snmp server 3955
snmp target 3956
snmp trap 3958
snmp trap-timestamps 3959
snmp user 3960
ss7-routing-domain 3962
suspend local-user 3964
system 3965
tacacs mode 3967
task facility ipsecmgr 3968
task facility sessmgr 3969
task facility acsmgr 3970
terminal 3971
threshold 10sec-cpu-utilization 3973
threshold aaa-acct-archive-queue-size 3974
threshold aaa-acct-archive-size 3976
threshold aaa-acct-failure 3978
threshold aaa-acct-failure-rate 3979

threshold aaa-auth-failure 3980
threshold aaa-auth-failure-rate 3981
threshold aaa-retry-rate 3983
threshold aaamgr-request-queue 3984
threshold asngw-auth-failure 3986
threshold asngw-handoff-denial 3988
threshold asngw-max-eap-retry 3989
threshold asngw-network-entry-denial 3991
threshold asngw-r6-invalid-nai 3992
threshold asngw-session-setup-timeout 3993
threshold asngw-session-timeout 3994
threshold call-reject-no-resource 3995
threshold call-setup 3996
threshold call-setup-failure 3997
threshold cpu-available-memory 3998
threshold cpu-load 4000
threshold cpu-memory-usage 4001
threshold cpu-orbs-crit 4003
threshold cpu-orbs-warn 4005
threshold cpu-session-throughput 4007
threshold cdr-file-space 4009
threshold contfilt-block 4011
threshold contfilt-rating 4012
threshold cpu-utilization 4013
threshold dcca-bad-answers 4015
threshold dcca-protocol-error 4017
threshold dcca-rating-failed 4019
threshold dcca-unknown-rating-group 4021
threshold diameter diameter-retry-rate 4023
threshold dns-learnt-ip-max-entries 4025
threshold edr-file-space 4027
threshold edr-udr-dropped flow control 4029
threshold fw-deny-rule 4031
threshold fw-dos-attack 4032
threshold fw-drop-packet 4033
threshold fw-no-rule 4034
threshold license 4035
threshold mgmt-cpu-memory-usage 4037
threshold mgmt-cpu-utilization 4039
threshold mme-attach-failure 4041
threshold mme-auth-failure 4043
threshold model 4045
threshold monitoring 4047
threshold nat-port-chunks-usage 4052
threshold packets-filtered-dropped 4053
threshold packets-forwarded-to-cpu 4054
threshold pdg-current-active-sessions 4056
threshold pdg-current-sessions 4057
threshold pdif-current-sessions 4058
threshold pdif-current-active-sessions 4059
threshold per-service-ggsn-sessions 4060
threshold per-service-gprs-pdp-sessions 4061
threshold per-service-gprs-sessions 4062
threshold per-service-ha-sessions 4063

threshold per-service-lns-sessions 4064
threshold per-service-pdsn-sessions 4065
threshold per-service-sgsn-pdp-sessions 4066
threshold per-service-sgsn-sessions 4067
threshold poll 4068
threshold poll aaa-acct-archive-queue-size 4084
threshold poll aaa-acct-archive-size 4085
threshold poll aaa-acct-failure 4086
threshold poll aaa-acct-failure-rate 4087
threshold poll aaa-auth-failure 4088
threshold poll aaa-auth-failure-rate 4089
threshold poll aaa-retry-rate 4090
threshold poll aaamgr-request-queue 4091
threshold poll asngw-auth-failure 4092
threshold poll asngw-handoff-denial 4093
threshold poll asngw-max-eap-retry 4094
threshold poll asngw-network-entry-denial 4095
threshold poll asngw-r6-invalid-nai 4096
threshold poll asngw-session-setup-timeout 4097
threshold poll asngw-session-timeout 4098
threshold poll cdr-file-space 4099
threshold poll contfilt-block 4100
threshold poll contfilt-rating 4101
threshold poll dcca-bad-answers 4102
threshold poll dcca-protocol-error 4103
threshold poll dcca-rating-failed 4104
threshold poll dcca-unknown-rating-group 4105
threshold poll diameter-retry-rate 4106
threshold poll edr-file-space 4107
threshold poll mme-attach-failure 4108
threshold poll mme-auth-failure 4109
threshold poll total-hnbgw-hnb-sessions 4110
threshold poll total-hnbgw-iu-sessions 4111
threshold poll total-hnbgw-ue-sessions 4112
threshold poll total-mme-sessions 4113
threshold poll port-rx-utilization 4114
threshold poll port-tx-utilization 4115
threshold poll port-high-activity 4116
threshold poll route-service 4117
threshold poll tpo-dns-failure 4118
threshold poll tpo-low-compression-gain 4119
threshold poll tpo-rto-timeout 4120
threshold ppp-setup-fail-rate 4121
threshold route-service bgp-routes 4122
threshold rp-setup-fail-rate 4124
threshold spc-cpu-memory-usage 4125
threshold spc-cpu-utilization 4126
threshold storage-utilization 4127
threshold subscriber active 4128
threshold subscriber total 4129
threshold total-ggsn-sessions 4130
threshold total-gprs-sessions 4131
threshold total-gprs-pdp-sessions 4132
threshold total-ha-sessions 4133

threshold total-hnbgw-hnb-sessions 4134
threshold total-hnbgw-iu-sessions 4136
threshold total-hnbgw-ue-sessions 4138
threshold total-hsgw-sessions 4140
threshold total-lma-sessions 4141
threshold total-lns-sessions 4142
threshold total-mme-sessions 4143
threshold total-pdsn-sessions 4144
threshold total-pgw-sessions 4145
threshold total-sgw-sessions 4146
threshold total-sgsn-sessions 4147
threshold total-sgsn-pdp-sessions 4148
threshold tpo-dns-failure 4149
threshold tpo-low-compression-gain 4150
threshold tpo-rto-timeout 4151
timestamps 4152
upgrade limit 4153
url-blacklisting database 4154

Global Title Translation Address-Map Configuration Mode Commands 4155

associate 4156
description 4157
end 4158
exit 4159
gt-address 4160
mode 4161
out-address 4162

Global Title Translation Association Configuration Mode Commands .. 4163

action 4164
description 4166
end 4167
exit 4168
gt-format 4169
variant 4170

GPRS Service Configuration Mode Commands 4171

accounting 4172
admin-disconnect-behavior 4174
associate-dscp-template 4176
associate-service 4177
cc profile 4178
check-imei 4180
check-imei-timeout-action 4181
ciphering-algorithm 4182
dns israu-mcc-mnc-encoding 4184
end 4185
exit 4186
gmm 4187
llc 4191
nri 4194
paging-policy 4196
peer-nsei 4198
plmn 4199
reporting-action event-record 4200

setup-timout 4201
sgsn-context-request 4202
sgsn-number 4203
sm 4204
sndcp 4206
GRE Tunnel Interface Configuration Mode Commands 4207
destination 4208
end 4209
exit 4210
keepalive 4211
source 4212
tos 4213
ttl 4215
Gs Service Configuration Mode Commands 4217
associate-sccp-network 4218
bssap+ 4219
end 4220
exit 4221
max-retransmission 4222
non-pool-area 4223
pool-area 4224
sgsn-number 4225
timeout 4226
vlr 4228
GT-Format1 Configuration Mode Commands 4229
end 4230
exit 4231
nature-of-address 4232
odd-even-indicator 4233
GT-Format2 Configuration Mode Commands 4235
end 4236
exit 4237
translation-type 4238
GT-Format3 Configuration Mode Commands 4239
encoding-scheme 4240
end 4241
exit 4242
numbering-plan 4243
translation-type 4244
GT-Format4 Configuration Mode Commands 4245
encoding-scheme 4246
end 4247
exit 4248
nature-of-address 4249
numbering-plan 4250
translation-type 4251
GTPP Server Group Configuration Mode Commands 4253
end 4254
exit 4255
gtpp attribute 4256

gtpp charging-agent 4260
gtpp data-request sequence-numbers 4261
gtpp deadtime 4262
gtpp dead-server suppress-cdrs 4263
gtpp detect-dead-server 4264
gtpp dictionary 4265
gtpp duplicate-hold-time 4267
gtpp echo-interval 4268
gtpp egcdr 4270
gtpp error-response 4272
gtpp max-cdrs 4273
gtpp max-pdu-size 4274
gtpp max-retries 4275
gtpp mbms bucket 4276
gtpp mbms interval 4277
gtpp mbms tariff 4278
gtpp mbms volume 4279
gtpp redirection-allowed 4280
gtpp redirection-disallowed 4281
gtpp server 4282
gtpp source-port-validation 4284
gtpp storage-server 4285
gtpp storage-server local file 4286
gtpp storage-server max-retries 4290
gtpp storage-server mode 4291
gtpp storage-server timeout 4293
gtpp suppress-cdrs zero-volume-and-duration 4294
gtpp timeout 4295
gtpp trigger 4296
gtpp transport-layer 4299

GTP-U Service Configuration Mode Commands 4301

bind 4302
echo-interval 4304
end 4305
exit 4306
extension-header 4307
ipsec-allow-error-ind-in-clear 4308
ipsec-tunnel-idle-timeout 4309
max-retransmissions 4310
path-failure detection-policy 4311
retransmission-timeout 4312
sequence-number 4313

HA Proxy DNS Configuration Mode Commands 4315

end 4316
exit 4317
pass-thru 4318
redirect 4319

HA Service Configuration Mode Commands 4321

a11-signalling-packets 4322
aaa 4323
access-network 4324
associate 4325

authentication 4326
bind 4328
encapsulation 4330
end 4331
exit 4332
fa-ha-spi 4333
gre 4335
idle-timeout-mode 4337
ikev1 4338
ip context-name 4339
ip local-port 4340
ip pool 4341
min-reg-lifetime 4342
mn-ha-spi 4343
nat-traversal 4345
optimize tunnel-reassembly 4346
per-domain statistics-collection 4347
policy bc-query-result 4348
policy nw-reachability-fail 4349
policy overload 4351
reg-lifetime 4353
reverse-tunnel 4354
revocation 4355
setup-timeout 4357
simul-bindings 4358
threshold dereg-reply-error 4359
threshold init-rrq-rcvd-rate 4360
threshold ipsec-call-req-rej 4361
threshold ipsec-ike-failrate 4362
threshold ipsec-ike-failures 4363
threshold ipsec-ike-requests 4364
threshold ipsec-tunnels-established 4365
threshold ipsec-tunnels-setup 4366
threshold reg-reply-error 4367
threshold rereg-reply-error 4368
wimax-3gpp2 interworking 4369

HD RAID Configuration Mode Commands 4371

end 4372
exit 4373
overwrite 4374
select 4375

HD Storage Policy Configuration Mode Commands 4377

directory 4378
end 4379
exit 4380
file 4381

HLR Configuration Mode Commands 4383

acn-version-retention 4385
end 4386
exit 4387
imsi 4388
policy routing 4390

HNB-GW Service Configuration Mode Commands 4391
access-control-db 4392
associate gtpu-service 4393
associate rtp pool 4394
end 4395
exit 4396
handin 4397
hnb-access-mode 4398
ip iu-qos-dscp 4400
ip iuh-qos-dscp 4403
paging open-hnb 4406
radio-network-plmn 4407
ranap reset 4409
rtcp report 4411
rtp mux 4412
sctp 4413
sctp bind 4417
sctp connection-timeout 4418
sctp heart-beat-timeout 4419
security-gateway aaa 4420
security-gateway bind 4422
security-gateway username 4424
tnnsf-timer 4425
ue registration-timeout 4426

HNB-CS Network Configuration Mode Commands 4427
associate alcap-service 4428
associate rtp pool 4430
associate sccp-network 4431
end 4432
exit 4433
map core-network-id 4434
map idnns 4435
map lac 4437
map nri 4439
msc deadtime 4441
msc point-code 4443
nri length 4444
null-nri 4445
offload-msc 4446

HNB-PS Network Configuration Mode Commands 4447
associate gtpu-service 4448
associate-sccp-network 4449
end 4450
exit 4451
map core-network-id 4452
map idnns range 4453
map nri range 4455
nri length 4457
null-nri 4458
offload-sgsn 4459
sgsn deadtime 4460
sgsn point-code 4462

HNB-RN PLMN Configuration Mode Commands 4463
associate cs-network 4464
associate ps-network 4465
end 4467
exit 4468
rnc-id 4469
HSGW Service Configuration Mode Commands 4471
a11-signalling-packets 4472
associate 4473
bind address 4474
context-retention-timer 4476
data-available-indicator 4477
data-over-signaling 4478
dns-pgw 4479
end 4480
exit 4481
fqdn 4482
fragment 4484
gre 4485
ip 4488
lifetime 4490
max-retransmissions 4491
mobile-access-gateway 4492
network-initiated-qos 4493
plmn id 4494
policy overload 4495
profile-id-qci-mapping 4497
registration-deny 4498
retransmission-timeout 4499
rsvp 4500
setup-timeout 4501
spi remote-address 4502
unauthorized-flows 4504
HSGW Service RoHC Configuration Mode Commands 4505
cid-mode 4506
end 4507
exit 4508
mrru 4509
profile 4510
HSS Peer Service Configuration Mode Commands 4511
auth-request 4512
diameter hss-dictionary 4513
diameter hss-endpoint 4514
end 4515
exit 4516
failure-handling 4517
request timeout 4519
IKEv2 Security Association Configuration Mode Commands 4521
default 4522
encryption 4523
end 4524

exit 4525
group 4526
hmac 4527
lifetime 4528
prf 4529
IMEI Profile Configuration Mode 4531
associate 4532
blacklist 4533
description 4534
direct-tunnel 4535
end 4536
exit 4537
ggsn-address 4538
IMS Authorization Service Configuration Mode Commands 4539
end 4540
exit 4541
p-cscf discovery 4542
p-cscf table 4544
policy-control 4546
qos-update-timeout 4547
signaling-flag 4548
signaling-flow 4549
traffic-policy 4550
IMS Sh Service Configuration Mode Commands 4551
diameter 4552
end 4553
exit 4554
failure-handling 4555
request 4557
IP VRF Context Configuration Mode Commands 4559
end 4560
exit 4561
ip maximum-routes 4562
mpls map-dscp-to-exp 4563
mpls map-exp-to-dscp 4565
IPMS Client Configuration Mode Commands 4567
end 4568
exit 4569
export keys 4570
heartbeat 4571
server 4572
source 4573
IPSec Transform Set Configuration Mode Commands 4575
encryption 4576
end 4578
exit 4579
group 4580
hmac 4582
mode 4583
IPSG RADIUS Server Configuration Mode Commands 4585

bind 4586
connection authorization 4588
end 4589
exit 4590
profile 4591
radius accounting 4592
radius dictionary 4594
setup-timeout 4596

IPSG RADIUS Snoop Configuration Mode Commands 4597

bind 4598
connection authorization 4599
end 4600
exit 4601
radius 4602
setup-timeout 4604

IPSP Configuration Mode Commands 4605

dead-interval 4606
end 4607
exit 4608
reserved-free-percentage 4609

IPv6 ACL Configuration Mode Commands 4611

deny/permit (by source IP address masking) 4612
deny/permit (any) 4614
deny/permit (by host IP address) 4616
deny/permit (by source ICMP packets) 4618
deny/permit (by IP packets) 4621
deny/permit (by TCP/UDP packets) 4624
end 4628
exit 4629
readdress server 4630
redirect context (by IP address masking) 4633
redirect context (any) 4635
redirect context (by host IP address) 4637
redirect context (by source ICMP packets) 4639
redirect context (by IP packets) 4642
redirect context (by TCP/UDP packets) 4645
redirect css delivery-sequence 4649
redirect css service (any) 4650
redirect css service (by host IP address) 4652
redirect css service (by ICMP packets) 4654
redirect css service (by IP packets) 4657
redirect css service (by source IP address masking) 4660
redirect css service (by TCP/UDP packets) 4662
redirect css service (for downlink, any) 4666
redirect css service (for downlink, by host IP address) 4668
redirect css service (for downlink, by ICMP packets) 4670
redirect css service (for downlink, by IP packets) 4674
redirect css service (for downlink, by source IP address masking) 4677
redirect css service (for downlink, by TCP/UDP packets) 4679
redirect css service (for uplink, any) 4683
redirect css service (for uplink, by host IP address) 4685
redirect css service (for uplink, by ICMP packets) 4687

redirect css service (for uplink, by IP packets) 4690
redirect css service (for uplink, by source IP address masking) 4693
redirect css service (for uplink, by TCP/UDP packets) 4695
redirect nexthop (by IP address masking) 4699
redirect nexthop (any) 4702
redirect nexthop (by host IP address) 4704
redirect nexthop (by source ICMP packets) 4706
redirect nexthop (by IP packets) 4710
redirect nexthop (by TCP/UDP packets) 4713

IPv6 to IPv4 Tunnel Interface Configuration Mode Commands 4717

destination address 4718
end 4719
exit 4720
mode 4721
source 4722
tos 4723
ttl 4724

ISAKMP Configuration Mode Commands 4725

authentication 4726
encryption 4727
end 4728
exit 4729
group 4730
hash 4731
lifetime 4732

IuPS Service Configuration Mode Commands 4733

access-protocol 4734
blacklist-timeout-gtpu-bind-addresses 4735
empty-cr 4736
end 4737
exit 4738
force-authenticate consecutive-security-failure 4739
gtpu 4741
iu-hold-connection 4743
iu-recovery 4744
iu-release-complete-timeout 4745
loss-of-radio-coverage ranap-cause 4746
mbms 4747
network-sharing cs-ps-coordination 4748
network-sharing failure-code 4749
plmn 4751
rab-assignment-response-timeout 4753
radio-network-controller 4754
relocation-alloc-timeout 4755
relocation-complete-timeout 4756
reset 4757
rnc 4759
security-mode-complete-timeout 4760
srns-context-response-timeout 4761
tigoc-timeout 4762
tintc-timeout 4763

LAC Service Configuration Mode Commands 4765

allow 4766
bind 4768
data sequence-number 4769
default 4770
end 4772
exit 4773
hide-attributes 4774
keepalive-interval 4775
load-balancing 4776
local-receive-window 4777
max-retransmission 4778
max-session-per-tunnel 4779
max-tunnel-challenge-length 4780
max-tunnels 4781
peer-lns 4782
proxy-lcp-authentication 4784
retransmission-timeout-first 4785
retransmission-timeout-max 4786
single-port-mode 4787
snoop framed-ip-address 4788
trap 4789
tunnel selection-key 4790
tunnel-authentication 4792

Line Configuration Mode Commands 4793

default 4794
end 4795
exit 4796
length 4797
width 4798

Link Configuration Mode Commands 4799

arbitration 4800
end 4801
exit 4802
mtp2-aerm-emergency-threshold 4803
mtp2-aerm-normal-threshold 4804
mtp2-eim-decrement 4805
mtp2-eim-increment 4806
mtp2-eim-threshold 4807
mtp2-error-correction 4808
mtp2-lssu-len 4809
mtp2-max-outstand-frames 4810
mtp2-suerm-threshold 4811
mtp3-discard-priority 4812
mtp3-max-slt-try 4813
mtp3-msg-priority 4814
mtp3-msg-size 4815
mtp3-p1-qlen 4816
mtp3-p2-qlen 4817
mtp3-p3-qlen 4818
mtp3-test-pattern 4819
priority 4820
signaling-link-code 4821
sscf-nni-n1 4822

sscop-max-cc 4823
sscop-max-pd 4824
sscop-max-stat 4825
timeout 4826

Linkset Configuration Mode Commands 4831

adjacent-point-code 4832
end 4833
exit 4834
link 4835
self-point-code 4836

LMA Service Configuration Mode Commands 4837

aaa accounting 4838
bind address 4839
end 4841
exit 4842
mobility-option-type-value 4843
refresh-advice-option 4844
refresh-interval-percent 4845
reg-lifetime 4846
revocation 4847
sequence-number-validate 4849
setup-timeout 4850
signalling-packets 4851
simul-bindings 4852
standalone 4853
timestamp-option-validation 4854
timestamp-replay-protection 4855

LNS Service Configuration Mode Commands 4857

aaa accounting 4858
authentication 4859
avp map called-number apn 4861
bind 4862
data sequence-number 4863
default 4864
end 4867
exit 4868
ip source-violation 4869
keepalive-interval 4871
local-receive-window 4872
max-retransmission 4873
max-session-per-tunnel 4874
max-tunnel-challenge-length 4875
max-tunnels 4876
nai-construction domain 4877
newcall 4878
peer-lac 4879
proxy-lcp-authentication 4881
retransmission-timeout-first 4882
retransmission-timeout-max 4883
setup-timeout 4884
single-port-mode 4885
trap 4886

tunnel-authentication 4887
tunnel-switching 4888
Local Policy Actiondef Configuration Mode Commands 4889
action 4890
end 4893
exit 4894
Local Policy Eventbase Configuration Mode Commands 4895
end 4896
exit 4897
rule 4898
Local Policy Ruledef Configuration Mode Commands 4901
condition 4902
end 4905
exit 4906
Local Policy Service Configuration Mode Commands 4907
actiondef 4908
end 4910
exit 4911
eventbase 4912
ruledef 4913
Loopback Interface Configuration Mode Commands 4915
crypto-map 4916
description 4917
end 4918
exit 4919
ip address 4920
ip vrf 4921
ipv6 address 4922
LTE Emergency Profile Configuration Mode Commands 4923
ambr 4924
apn 4925
end 4926
exit 4927
pgw 4928
qos 4930
ue-validation-level 4931
LTE Forbidden Location Area Configuration Mode Commands 4933
end 4934
exit 4935
lac 4936
LTE Forbidden Tracking Area Configuration Mode Commands 4937
end 4938
exit 4939
tac 4940
LTE Handover Restriction List Configuration Mode Commands 4941
end 4942
exit 4943
forbidden 4944

LTE Network Global MME ID Management Database Configuration Mode Commands 4947
end 4948
exit 4949
plmn 4950
LTE Policy Configuration Mode Commands 4951
end 4952
exit 4953
ho-restrict-list 4954
lte-emergency-profile 4955
network-global-mme-id-mgmt-db 4956
subscriber-map 4957
tai-mgmt-db 4958
LTE Subscriber Map Configuration Mode Commands 4959
end 4960
exit 4961
precedence 4962
LTE TAI Management Database Configuration Mode Commands 4965
end 4966
exit 4967
tai-mgmt-obj 4968
timezone 4969
LTE TAI Management Object Configuration Mode Commands 4971
end 4972
exit 4973
lai 4974
sgw-address 4975
tai 4976
timezone 4977
zone-code 4978
MAG Service Configuration Mode Commands 4979
bind address 4980
encapsulation 4982
end 4983
exit 4984
information-element-set 4985
max-retransmissions 4986
mobility-option-type-value 4987
reg-lifetime 4988
renew-percent-time 4989
retransmission-policy 4990
retransmission-timeout 4991
signalling-packets 4992
MAP Service Configuration Mode Commands 4993
access-protocol 4994
application-context-name 4995
auth-vectors 4997
end 4998
equipment-identity-register 4999
exit 5001

hlr 5002
policy 5003
short-message-service 5004
MIP HA Assignment Table Configuration Mode Commands 5005
end 5006
exit 5007
hoa-range 5008
MIPv6HA Service Configuration Mode Commands 5009
aaa accounting 5010
bind 5011
default 5012
end 5014
exit 5015
refresh-advice-option 5016
refresh-interval-percent 5017
reg-lifetime 5018
sequence-number-validate 5019
setup-timeout 5020
simul-bindings 5021
timestamp-replay-protection tolerance 5022
MME LAC Pool Area Configuration Mode Commands 5023
end 5024
exit 5025
hash-value 5026
lac 5028
plmn-id 5029
MME Service Configuration Mode Commands 5031
associate 5032
bind s1-mme 5035
csg-change-notification 5037
dns 5038
emm 5040
enb-cache-timeout 5048
encryption-algorithm-lte 5049
end 5051
esm 5052
exit 5055
gtpv2 5056
heuristic-paging 5057
integrity-algorithm-lte 5058
location-reporting 5060
max-bearers per-subscriber 5061
max-paging-attempts 5062
max-pdns per-subscriber 5063
mme-id 5064
mmemgr-recovery 5065
msc 5066
nas-max-retransmission 5067
network-sharing 5068
nri 5069
peer-mme 5070
peer-sgsn 5072

pgw-address 5074
plmn-id 5076
policy attach 5077
policy idle-mode 5079
policy inter-rat 5080
policy network 5081
policy overload 5082
policy pdn-reconnection 5083
policy s1-reset 5084
policy sctp-down 5085
policy tau 5086
relative-capacity 5088
s1-mme ip 5089
s1-mme sctp port 5090
setup-timeout 5091
snmp trap 5092
ue-db 5093

MME SGs Service Configuration Mode Commands 5095

associate 5096
bind 5097
end 5098
exit 5099
non-pool-area 5100
pool-area 5102
sctp 5103
tac-to-lac-mapping 5104
timer 5105
vlr 5106

MPLS-IP Configuration Mode Commands 5107

end 5108
exit 5109
protocol 5110

MPLS-LDP Configuration Mode Commands 5111

advertise-labels 5112
discovery 5113
enable 5114
end 5115
exit 5116
router-id 5117
session 5118

MSEG APN Profile Configuration Mode Commands 5119

apn 5120
end 5121
exit 5122

MSEG Associated Services Profile Configuration Mode Commands 5123

active-charging-rulebase 5124
end 5125
exit 5126
fw-nat-policy 5127
ip 5128

MSEG Criteria Configuration Mode Commands 5129

end 5130
exit 5131
filter priority 5132
MSEG Global Configuration Mode Commands 5135
apn-profile 5136
associated-services-profile 5137
end 5138
exit 5139
imei-profile 5140
imsi-profile 5141
mseg-criteria 5142
mseg-ruleset 5143
peer-mseg-profile 5144
rnc-profile 5145
MSEG IMEI Profile Configuration Mode Commands 5147
end 5148
exit 5149
imei-range 5150
MSEG IMSI Profile Configuration Mode Commands 5151
end 5152
exit 5153
imsi-range 5154
MSEG Peer Profile Configuration Mode Commands 5155
end 5156
exit 5157
mseg-gtpc 5158
mseg-gtpu 5159
mseg-id 5160
MSEG RNC Profile Configuration Mode Commands 5161
associate 5162
end 5163
exit 5164
location 5165
rnc-gtpu 5166
rnc-id 5167
MSEG Ruleset Configuration Mode Commands 5169
apn 5170
end 5171
exit 5172
imei 5173
imsi 5174
MSEG Service Configuration Mode Commands 5175
associate 5176
bind gtpc-address 5177
bind gtpu-address 5178
end 5179
exit 5180
gtpc 5181
gtpu 5183
mseg-criteria 5185

mseg-id 5186
path-failure 5187
Network Service Entity - Peer NSEI Configuration Mode Commands 5189
bssgp-timer 5190
end 5191
exit 5192
ns-reset-mode 5193
ns-vc 5194
Network Service Entity- IP Local Configuration Mode Commands..... 5195
all-nsvc-failure-action 5196
bssgp-timer 5197
end 5198
exit 5199
max-ns-retransmissions 5200
ns-timer 5201
nsvc-failure-action 5202
nsvl 5203
peer-network-service-entity 5204
retry-count 5205
timer 5206
Network Service Virtual Connection Configuration Mode Commands .. 5207
end 5208
exit 5209
Network Service Virtual Link Configuration Mode Commands 5211
end 5212
exit 5213
nsvl-address 5214
weight 5215
NTP Configuration Mode Commands 5217
enable 5218
end 5219
exit 5220
server 5221
Operator Policy Configuration Mode 5223
apn 5224
associate 5225
description 5226
end 5227
exit 5228
imei 5229
ORBEM Configuration Mode Commands 5231
activate 5232
client 5233
default 5234
end 5236
event-notif-iiop-port 5237
event-notif-service 5238
event-notif-siop-port 5246
exit 5247
iiop-port 5248

iiop-transport 5249
iop-address 5250
max-attempt 5251
session-timeout 5252
siop-port 5253
ssl-auth-policy 5254
ssl-certificate 5255
ssl-private-key 5257

OSPF Configuration Mode Commands 5259

area authentication 5260
area default-cost 5261
area nssa 5262
area stub 5263
area virtual-link 5264
area virtual link authentication 5265
area virtual-link authentication-key 5267
area virtual link intervals 5268
area virtual link message-digest-key 5270
capability graceful-restart 5272
default-information originate 5273
default metric 5274
distance 5275
distribute-list 5276
end 5277
exit 5278
ip vrf 5279
neighbor 5280
network area 5281
ospf graceful-restart 5282
ospf router-id 5283
passive-interface 5284
redistribute 5285
refresh timer 5286
router-id 5287
timers spf 5288

OSPFv3 Configuration Mode Commands 5289

area 5290
default-metric 5292
end 5293
exit 5294
passive Interface 5295
redistribute 5296
router-id 5297
timers spf 5298

OSPF VRF Configuration Mode Commands 5299

area 5300
default-information originate 5304
default metric 5305
distance 5306
distribute-list 5307
end 5308
exit 5309

neighbor 5310
network area 5311
ospf router-id 5312
passive-interface 5313
redistribute 5314
refresh timer 5315
router-id 5316
timers spf 5317

Out-Address Configuration Mode Commands 5319

end 5320
exit 5321
gt-address 5322
gt-format 5323
ni-indicator 5324
point-code 5325
routing-indicator 5326
ssf 5327
ssn 5328

PCC-Action-Set Configuration Mode Commands 5329

af-media-type 5330
associate monitoring-key 5332
authorize 5333
dissociate monitoring-key 5335
dynamic-rule-install 5336
dynamic-rule-uninstall 5340
end 5341
exit 5342
log-event 5343
notify-user 5344
offline-charging-server 5345
online-charging-server 5346
request-usage-report monitoring-key 5347
rule-activate 5348
rule-deactivate 5349
rulebase-activate 5350
rulebase-deactivate 5351
service-tag 5352
terminate-session 5353
usage-monitor 5354

PCC-AF-Service Configuration Mode Commands 5355

associate pcc-service 5356
diameter dictionary 5357
diameter origin end-point 5358
end 5359
exit 5360

PCC-Condition-Group Configuration Mode Commands 5361

af-application-id 5362
af-media-codec 5363
af-media-type 5365
af-service-urn 5367
an-gw-address 5368
authorized-qci 5370

base-station-id 5371
bearer-count 5373
connectivity-access-network 5374
end 5376
eval-condition-group 5377
eval-condition-group 5379
event-time 5381
event-trigger 5382
imsi 5384
msisdn 5385
multi-line-or 5386
nai 5387
out-of-credit rulename 5388
out-of-credit rulebase-name 5389
pcef-address 5390
pdn-id 5392
profile-attribute 5393
radio-access-technology 5394
sgsn-ip 5396
sgsn-mcc-mnc 5398
subscription-attribute 5399
spr-profile-not-found 5400
threshold-condition usage-monitor 5401
user-access-network 5403
user-equipment-info esn 5404
user-equipment-info eui64 5405
user-equipment-info imeisv 5406
user-equipment-info mac 5407
user-equipment-info meid 5408
user-equipment-info modified-eui64 5409
user-location-info 5410

PCC-Data-Service Configuration Mode Commands 5413

end 5414
exit 5415
flow direction in 5416
flow direction out 5418
metering-method 5420
monitoring-key 5421
precedence 5422
qos-profile 5423
rating-group 5424
reporting-level 5425
service-identifier 5426

PCC-Event-Notification-Interface-Endpoint Configuration Mode Commands 5427

address 5428
end 5429
exit 5430
peer name 5431
peer select-algorithm 5432
peer select-peer 5433

PCC-Policy-Service Configuration Mode Commands 5435

associate pcc-service 5436

diameter dictionary 5437
diameter origin end-point 5438
ehrpd-access-bcm 5439
end 5440
exit 5441
gprs-access-bcm 5442
max policy-sessions 5443
subscriber-binding-identifier 5444
subscription-id-absence-action 5445
unsolicited-provisioning 5446

PCC-QoS-Profile Configuration Mode Commands 5447

arp-priority 5448
end 5450
exit 5451
guaranteed-bitrate 5452
max-bitrate 5453
qci 5454

PCC-Service-Profile Configuration Mode Commands 5455

default-rulebase-name 5456
end 5457
eval-priority 5458
exit 5460
service-tag 5461
usage-monitor 5463
unknown-services-treatment 5465

PCC-Service Configuration Mode Commands 5467

action-set 5468
charging method 5469
charging server 5470
condition-group 5472
data-service 5474
end 5476
exit 5477
map-profile priority 5478
monitoring-key 5480
multiple-pcef-per-subscriber 5482
profile 5483
qos-profile 5485
spr-failure 5487
ssc-usage-update-policy 5488
timedef 5489
timeout idle 5491
timeout setup 5493

PCC-Sp-Endpoint Configuration Mode Commands 5495

access-type 5496
diameter dictionary 5497
diameter origin end-point 5498
diameter peer-select 5499
end 5501
exit 5502
profile-data 5503
profile-update-notification 5505

spr subscriber identifier 5506
PCC-TimeDef Configuration Mode Commands 5509
end 5510
exit 5511
start date 5512
start day 5514
start time 5516
PCC-Usage-Monitor Configuration Mode Commands 5517
end 5518
exit 5519
usage-limit volume 5520
PDG Service Configuration Mode Commands 5521
aaa attribute 5522
associate sgtp-service 5523
certificate-selection 5524
bind 5525
ip gnp-qos-dscp 5527
ip qos-dscp 5530
ip source-violation 5533
max-tunnels-per-ue 5535
plmn id 5536
setup-timeout 5537
PDIF Service Configuration Mode Commands 5539
aaa attribute 5540
aaa authentication 5542
bind 5544
default 5545
duplicate-session-detection 5547
end 5548
exit 5549
hss 5550
ims-sh-service 5552
ip source-violation 5553
mobile-ip 5554
setup-timeout 5555
username 5556
PDSN Service Configuration Mode Commands 5557
a11-signalling-packets 5558
aaa 3gpp2-service-option 5559
aaa nas-ip-address 5560
access-flow traffic-validation 5561
access-network 5562
airlink bad-sequence-number 5563
allow alt-ppp 5564
always-on-indication 5565
associate 5566
authentication 5567
bcmcs 5569
bind 5571
data-available-indicator 5573
data-over-signaling 5574

default subscriber 5575
direct-lte-indicator 5576
dormant-transition 5577
end 5578
exit 5579
fragment 5580
gre 5581
inter-pdsn-handoff mobility-event-indicator 5584
inter-pdsn-handover 5585
ip header-compression rohc 5586
ip local-port 5587
ip source-violation 5588
lifetime 5590
max-retransmissions 5591
mobile-ip foreign-agent context 5592
mobile-ipv6 5593
msid length 5594
nai-construction 5595
new-call conflict 5596
pcf-monitor 5597
pcf-session-id-change restart-ppp 5599
pdsn type0-tft attempt-inner-match 5600
peer-pcf 5601
pma-capability-indicator 5602
policy 5603
ppp 5606
qos-profile-id-mapping 5608
qos update 5610
registration-accept 5611
registration-ack-deny terminate-session-on-error 5612
registration-deny 5613
registration-discard 5615
registration-update 5617
retransmission-timeout 5618
service-option 5619
setup-timeout 5621
simple-ip allow 5622
spi 5623
tft-validation wait-timeout 5626
threshold a11-ppp-send-discard 5627
threshold a11-rac-msg-discard 5628
threshold a11-rrp-failure 5629
threshold a11-rrq-msg-discard 5630
threshold init-rrq-rcvd-rate 5631

PDSN Service RoHC Configuration Mode Commands 5633

cid-mode 5634
end 5635
exit 5636
mrru 5637
profile 5638

Peer-Server Configuration Mode Commands 5639

end 5640
exit 5641

mode 5642
name 5643
psp 5644
routing-context 5645
self-point-code 5646

P-GW Service Configuration Mode Commands 5647

associate 5648
authorize-with-hss 5650
dns-client 5651
end 5652
exit 5653
fqdn 5654
gx-li 5656
newcall 5657
plmn 5658
session-delete-delay 5659

Policy Control Configuration Mode Commands 5661

apn-name-to-be-included 5662
arp-priority-level 5663
cc-profile 5664
custom-reauth-trigger 5666
diameter dictionary 5668
diameter host-select reselect 5670
diameter host-select row-precedence 5671
diameter host-select table 5674
diameter origin endpoint 5676
diameter request-timeout 5677
diameter update-dictionary-avps 5678
end 5680
event-report-indication 5681
event-update 5682
exit 5683
failure-handling 5684
li-secret 5687

PVC Configuration Mode Commands 5689

bind 5690
encapsulation aal5 5691
end 5692
exit 5693
shaping 5694
shutdown 5696

PVC Interface Configuration Mode Commands 5697

description 5698
end 5699
exit 5700
ip 5701
ip access-group 5702
ip address 5703
ip mtu 5704
ip ospf authentication-key 5705
ip ospf authentication-type 5706
ip ospf cost 5707

ip ospf dead-interval 5708
ip ospf hello-interval 5709
ip ospf message-digest-key 5710
ip ospf network 5711
ip ospf priority 5712
ip ospf retransmit-interval 5713
ip ospf transmit-delay 5714
QCI - QoS Mapping Configuration Mode Commands 5715
end 5716
exit 5717
qci 5718
QCI - RAN ID Mapping Configuration Mode Commands 5721
end 5722
exit 5723
profile-id 5724
Remote Address List Configuration Mode Commands 5727
address 5728
end 5729
exit 5730
RNC Configuration Mode Commands 5731
associate-gtpu-bind-address 5732
description 5733
direct-tunnel 5734
dual-address-pdp 5735
end 5737
exit 5738
lac 5739
mbms 5740
overload-action disable 5741
paging-non-searching-indication 5743
pointcode 5744
pooled 5745
rab-modify-procedure 5746
ranap global-cn-id 5747
ranap paging-area-id 5749
ranap paging-cause-ie 5750
ranap signalling-indication-ie 5753
ran-information-management 5754
release-compliance 5755
reset-resource 5757
RoHC Profile Common Options Configuration Mode Commands 5759
delay-release-hc-context-timer 5760
end 5761
exit 5762
inactive-traffic-release-hc-context-timer 5763
RoHC Profile Compression Configuration Mode Commands 5765
context-timeout 5766
end 5767
exit 5768
ipid-history-size 5769
max-jitter-cd 5770

max-sliding-window 5771
multiple-ts-stride 5772
new-context-blocking-time 5773
num-pkts-ts 5774
num-pkts-u-mode 5775
num-updates-ir 5776
optimistic-repeats 5777
rtp-sn-p 5778
rtp-sn-p-override 5779
rtp-time-stride 5780
rtp-ts-deviation 5781
rtp-ts-stride 5782
sliding-window-ts 5783
total-jitter-ipv4 5784
total-jitter-ipv6 5785
unimode-timeout-to-fo-state 5786
unimode-timeout-to-ir-state 5787
use-calculated-rtp-time-stride 5788
use-calculated-rtp-ts-stride 5789
use-ipid-override 5790
use-optimized-talkspurt 5791
use-optimized-transience 5792
use-timer-based-compression 5793
use-uncomp-profile 5794

RoHC Profile Configuration Mode Commands 5795

common-options 5796
compression-options 5797
decompression-options 5798
end 5799
exit 5800

RoHC Profile Decompression Configuration Mode Commands 5801

accept-delayed-pkts 5802
context-timeout 5803
crc-errors-fo 5804
crc-errors-so 5805
end 5806
exit 5807
nack-limit 5808
optimistic-mode-ack 5809
optimistic-mode-ack-limit 5810
piggyback-wait-time 5811
preferred-feedback-mode 5812
rtp-sn-p 5813
rtp-sn-p-override 5814
sliding-window-ts 5815
use-clock-option 5816
use-crc-option 5817
use-feedback 5818
use-jitter-option 5819
use-reject-option 5820
use-sn-not-valid-option 5821
use-sn-option 5822

Route-map Configuration Mode Commands 5823
end 5824
exit 5825
match as-path 5826
match interface 5827
match ip address 5828
match ip next-hop 5829
match metric 5830
match origin 5831
match route-type external 5832
match tag 5833
set as-path 5834
set ip next-hop 5835
set metric 5836
set metric-type 5837
set origin 5838
set tag 5839
set weight 5840

RS-232 Port Configuration Mode Commands 5841
default 5842
end 5843
exit 5844
preferred slot 5845
snmp trap link-status 5846
terminal 5847

SCCP Network Configuration Mode Commands 5849
associate 5850
description 5851
destination 5852
end 5854
exit 5855
global-title-translation 5856
hop-count 5857
self-point-code 5858
timeout 5859

SCTP Parameter Template Configuration Mode Commands 5861
sctp-alpha 5862
sctp-alt-accept-flag 5863
sctp-beta 5864
sctp-checksum-type 5865
sctp-cookie-life 5866
sctp-max-assoc-retx 5867
sctp-max-in-strms 5868
sctp-max-init-retx 5869
sctp-max-mtu-size 5870
sctp-max-out-strms 5871
sctp-max-path-retx 5872
sctp-min-mtu-size 5873
sctp-rto-initial 5874
sctp-rto-max 5875
sctp-rto-min 5876
sctp-sack-frequency 5877

sctp-sack-period 5878
sctp-start-mtu-size 5879
timeout 5880
Service Redundancy Protocol Configuration Mode Commands 5881
bind 5882
chassis-mode 5883
checkpoint 5884
configuration-interval 5885
dead-interval 5886
delay-interval 5887
end 5888
exit 5889
hello-interval 5890
internal-switchover-retry-interval 5891
monitor authentication-probe 5892
monitor bfd 5893
monitor bgp 5894
monitor diameter 5895
num-internal-switchover-retry 5897
peer-ip-address 5898
priority 5899
route-modifier 5900
Session Event Module Configuration Mode Commands 5901
end 5902
event 5903
exit 5906
file 5907
SGSN ASP Configuration Mode Commands 5911
end 5912
end-point 5913
exit 5915
SGSN Global Configuration Mode Commands 5917
aggregate-ipc-msg 5918
apn-resolve-dns-query snaptr 5920
bssgp-message ms-flow-control-from-unknown-ms 5921
bssgp-message ptp-bvc-reset 5922
bssgp-timer 5923
bvc-unblock 5924
dscp-template 5925
dual-address-pdp 5926
end 5928
exit 5929
gmm-message 5930
imsi-range 5931
map-message 5933
max-pending-attaches 5934
old-tlli invalidate tlli 5935
old-tlli hold-time 5936
pdp-deactivation-rate 5937
ranap excess-len ignore 5939
ran-information-management 5940
target-offloading 5941

tlli-cb-audit 5942
umts-aka-r99 5943
SGSN Pool Area Configuration Mode Commands 5945
end 5947
exit 5948
hash-value 5949
lac 5951
SGSN PSP Configuration Mode Commands 5953
associate 5954
end 5955
end-point 5956
exchange-mode 5957
exit 5958
psp-mode 5959
routing-context 5960
sctp-alpha 5962
sctp-beta 5963
sctp-checksum-type 5964
sctp-cookie-life 5965
sctp-init-rwnd 5966
sctp-max-assoc-retx 5967
sctp-max-init-retx 5968
sctp-max-mtu size 5969
sctp-max-out-strms 5970
sctp-max-path-retx 5971
sctp-rto-initial 5972
sctp-rto-max 5973
sctp-rto-min 5974
sctp-sack-frequency 5975
sctp-sack-period 5976
sctp-suppress-alarm 5977
timeout 5978
SGSN Service Configuration Mode Commands 5981
accounting 5982
admin-disconnect-behavior 5984
cc profile 5985
check-imei 5987
check-imei-timeout-action 5988
core-network 5989
disable/enable super-charger 5990
dns israu-mcc-mnc-encoding 5991
end 5992
exit 5993
gmm 5994
gs-service 5997
lac 5998
max-pdp-contexts 5999
mobile-application-part 6000
network-sharing cs-ps-coordination 6001
nri length 6002
override-lac-li 6004
override-rac-li 6005

rac 6006
ran-protocol 6007
reporting-action event-record 6008
sgsn-number 6009
sgtp-service 6010
sm 6011

SGTP Service Configuration Mode Commands 6013

direct-tunnel-disabled-ggsn 6014
disable-remote-restart-counter-verification 6015
end 6017
exit 6018
ggsn-fail-retry-timer 6019
gn-delay-monitoring 6020
gtpc 6022
gtpu 6025
ignore-remote-restart-counter-change 6027
max-remote-restart-counter-change 6028
mbms 6030
path-failure 6031
pool 6032

S-GW Service Configuration Mode Commands 6035

accounting context 6036
accounting mode 6037
associate 6038
ddn 6040
egtp-service 6041
end 6042
exit 6043
gtpu-error-ind 6044
mag-service 6046
path-failure 6047
plmn 6048
reporting-action 6049

SMS Service Configuration Mode Commands 6051

cp-data 6052
end 6053
exit 6054
mo-message-forwarding-destination 6055
smsc-address-restiction-list 6056
smsc-address-restiction-type 6057
smsc-address-selection-prioritization 6058
smsc-routing 6059
timeout 6060

SS7 Routing Domain Configuration Mode Commands 6061

asp 6062
description 6063
end 6064
exit 6065
inbound-asp-identifier validate 6066
linkset 6067
MTU-size 6068
peer-server 6069

route 6070
routing-context 6071
ssf 6072
SSH Configuration Mode Commands 6073
authorized-key 6074
end 6075
exit 6076
listen 6077
max servers 6078
subsystem 6079
SSL Template Configuration Mode Commands 6081
ca-certificate 6082
certificate 6083
cipher-suites 6084
end 6085
exit 6086
version 6087
Subscriber Configuration Mode Commands 6089
aaa 6090
access-link ip-fragmentation 6092
accounting-mode 6093
active-charging bandwidth-policy 6095
active-charging link-monitor tcp 6096
active-charging rulebase 6098
always-on 6099
asn-header-compression-rohc 6100
asn nspid 6101
asn-pdfid 6102
asn-policy 6103
authorized-flow-profile-id 6105
content-filtering category 6106
credit-control-group 6107
credit-control-service 6108
cscf core-service 6109
cscf county-name 6110
cscf nat-applicable 6111
cscf private-user-id 6112
cscf session-template 6113
data-tunneling ignore df-bit 6114
dcca origin host 6115
dcca origin endpoint 6116
dcca peer-select 6117
default 6118
dns 6121
eap 6122
encrypted password 6123
end 6124
exit 6125
external-inline-server 6126
firewall policy 6127
fw-and-nat policy 6128
idle-timeout-activity 6129

ims application-manager 6130
ims-auth-service 6131
inter-pdsn-handoff 6132
ip access-group 6133
ip address 6134
ip address pool 6135
ip address secondary-pool 6136
ip allowed-dscp 6137
ip context-name 6140
ip header-compression 6141
ip hide-service-address 6144
ip local-address 6145
ip multicast discard 6146
ip qos-dscp 6147
ip route 6149
ip source-validation 6150
ip user-datagram-tos copy 6151
ip vlan 6152
ipv6 access-group 6153
ipv6 address 6154
ipv6 dns 6155
ipv6 dns-proxy 6156
ipv6 egress-address-filtering 6157
ipv6 initial-router-advt 6158
ipv6 interface-id 6160
ipv6 minimum-link-mtu 6161
ipv6 secondary-address 6162
l2tp send accounting-correlation-info 6163
l3-to-l2-tunnel address-policy 6164
loadbalance-tunnel-peers 6165
long-duration-action 6166
max-pdn-connections 6168
mediation-device 6169
mobile-ip 6170
mobile-ip ha 6173
mobile-ip reg-lifetime-override 6174
mobile-ip send accounting-correlation-info 6175
mobile-ipv6 6176
nai-construction-domain 6177
nbns 6178
nexthop-forwarding-address 6179
npu qos 6180
nw-reachability-server 6181
outbound 6182
overload-disconnect 6183
password 6184
pdif mobile-ip 6185
permission 6186
policy ipv6 tunnel 6187
policy-group 6188
ppp 6189
prepaid 3gpp2 6192
prepaid custom 6194
prepaid unclassify 6196

prepaid voice-push 6197
prepaid wimax 6198
proxy-dns intercept list-name 6199
proxy-mip 6200
qos rate-limit 6201
qos traffic-police 6205
qos traffic-shape 6207
radius accounting 6210
radius group 6212
radius returned-framed-ip-address 6213
rohc-profile-name 6214
secondary ip pool 6215
simultaneous 6216
timeout 6217
timeout long-duration 6218
tpo policy 6219
tunnel address-policy 6220
tunnel ipip 6221
tunnel ipsec 6222
tunnel l2tp 6223

TACACS+ Configuration Mode Commands 6225

accounting 6226
authorization 6227
end 6228
exit 6229
on-authen-fail 6230
on-network-error 6231
on-unknown-user 6232
server 6233

Telnet Configuration Mode Commands 6235

end 6236
exit 6237
max servers 6238

TFTP Configuration Mode Commands 6239

end 6240
exit 6241
max servers 6242

Traffic Policy Group Configuration Mode Commands 6243

end 6244
exit 6245
policy 6246

Traffic Policy-Map Configuration Mode Commands 6247

3gpp2 data-over-signaling 6248
access-control 6249
accounting suppress 6250
accounting trigger 6251
class-map 6253
end 6254
exit 6255
flow-tp-trigger 6256
ip header-compression 6257

qos encaps-header 6258
qos traffic-police 6259
qos user-datagram dscp-marking 6261
sess-tp-trigger 6262
type 6263

Tunnel Interface Configuration Mode Commands 6265

description 6266
end 6267
exit 6268
ip address 6269
ipv6 address 6270
tunnel-mode 6271

UDR Format Configuration Mode Commands 6273

attribute 6274
end 6279
event-label 6280
exit 6281
rule-variable 6282

UDR Module Configuration Mode Commands 6285

cdr 6286
end 6290
exit 6291
file 6292

Video Group Configuration Mode 6297

end 6298
exit 6299
keepalive-server 6300
local-address 6302
server 6303

VLAN Configuration Mode Commands 6305

bind interface 6306
end 6307
exit 6308
ingress-mode 6309
priority 6310
shutdown 6311
vlan-map 6312

About this Guide

This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5x00 Chassis.

This preface includes the following sections:

- Conventions Used
- Contacting Customer Support
- Additional Information

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electrostatic Discharge (ESD)	Warns you to take proper grounding precautions before handling ESD sensitive components or devices.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents text that appears on your terminal screen, for example: `Login:`
Text represented as **`commands`**	This typeface represents commands that you enter at the CLI, for example: **`show ip access-list`** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **`command`** *`variable`*	This typeface represents a variable that is part of a command, for example: **`show card`** *`slot_number`* *`slot_number`* is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**.

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by braces. They must be entered as part of the command syntax.
[**`keyword`** or *`variable`*]	Optional keywords or variables that may or may not be used are surrounded by brackets.

Command Syntax Conventions	Description
|	Some commands support alternative variables. These "options" are documented within braces or brackets by separating each variable with a vertical bar. These variables can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

Contacting Customer Support

Go to http://www.cisco.com/cisco/web/support/ to submit a service request. A valid Cisco account (username and password) is required to access this site. Please contact your Cisco account representative for additional information.

Additional Information

Refer to the following guides for supplemental information about the system:

- *Command Line Interface Reference*
- *Statistics and Counters Reference*
- *Thresholding Configuration Guide*
- *SNMP MIB Reference*
- *Cisco Web Element Manager Installation and Administration Guide*
- Product-specific and feature-specific administration guides
- *Release Notes* that accompany updates and upgrades to StarOS

Chapter 1
Command Line Interface Overview

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

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

This section provides the following information about the CLI:

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

CLI Structure

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

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

CLI Command Modes

There are two primary CLI command modes:

- **Exec (Execute) Mode:** The Exec Mode is the lowest level in the CLI. The Exec Mode is where you execute basic commands such as **show** and **ping**. When you log into the CLI, you are placed in this mode by default.
- **Config (Configuration) Mode:** The Config mode is accessible only by users with administrator and security administrator privileges. If you are an administrative user, in this mode you can add and configure contexts and access the configuration sub-modes to configure protocols, interfaces, ports, services, subscribers, and other service-related items.

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

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

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

CLI Administrative Users

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

Administrative User Types

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

- **Context-level administrative users:** This user type is configured at the context-level and relies on the AAA subsystems for validating user names and passwords during login. This is true for both administrative user accounts configured locally through a configuration file or on an external RADIUS server. Passwords for these user types are assigned once and are accessible in the configuration file.
- **Local-users:** This user type provides support for ANSI T1.276-2003 password security protection. Local-user account information, such as passwords, password history, and lockout states, is maintained in non-volatile memory on the CompactFlash module and in the Shared Configuration Task (SCT). This information is maintained in a separate file, not in configuration files used by the system. As such, the configured local-user accounts are not visible with the rest of the system configuration.

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

Authenticating Administrative Users with RADIUS

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

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

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

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

The default value is 1 (CLI).

RADIUS Mapping System

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

Table 1. RADIUS Attribute/Value Mapping System

Attribute	Value
Framed	2
Administrative (Administrator)	6
NAS_Prompt	7
Authenticate_Only	8
Authorize_Only	17
Inspector	19650516
Security_Admin	19660618

RADIUS Privileges

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

Table 2. CLI Privilege Roles and RADIUS Service Types

CLI Configuration Parameter	RADIUS Service Type	show admin Type
administrator	Security_Admin (19660618)	admin
config_administrator	Administrative (6)	cfgadm
operator	NAS_Prompt (7)	oper
inspector	Inspector (19650516)	inspect

Administrative User Privileges

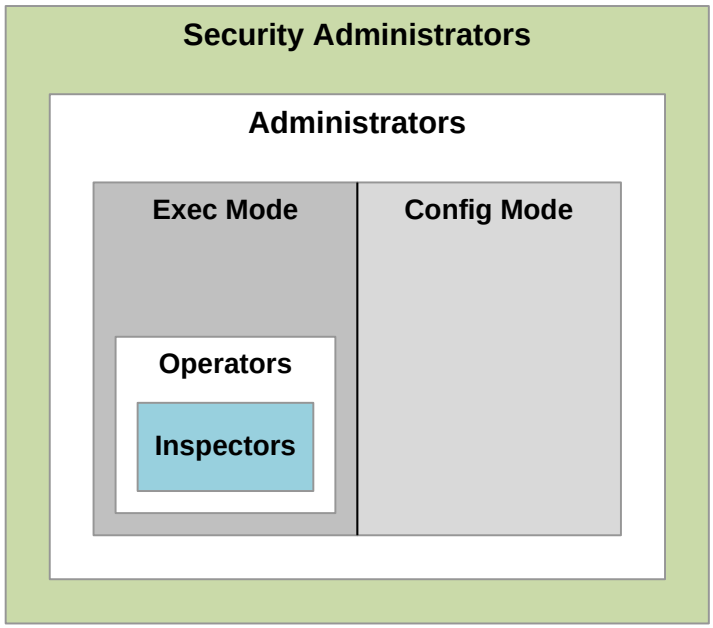
Regardless of the administrative user type, the system supports four user privilege levels:

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

- **Operator**: Operators have read-only privileges to a larger subset of the Exec Mode commands. They can execute all commands that are part of the inspector mode, plus some system monitoring, statistic, and fault management functions. Operators do not have the ability to enter the Config Mode.
- **Administrator**: Administrators have read-write privileges and can execute any command in the CLI except for a few security-related commands that can only be configured by Security Administrators. Administrators can configure or modify system settings and can execute all system commands, including those available to the Operators and Inspectors.
- **Security Administrator**: Security Administrators have read-write privileges and can execute all CLI commands, including those available to Administrators, Operators, and Inspectors.

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

Figure 1. User Privileges



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

Table 3. User Privilege to User Type Mapping

User Type as Defined by T1.276-2003	Local-User Level User	Context-Level User
System Security Administrator	Security Administrator	Administrator
Application Security Administrator	Security Administrator	Administrator
System Administrator	Administrator	Config-Administrator
Application Administrator	Administrator	Config-Administrator
Application User/Operator	Operator	Operator
not applicable	Inspector	Inspector

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

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

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

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

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

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

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

Allowed Commands per User Type

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

Inspector Mode Commands

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

- **abort**
- **autoconfirm**
- **context**
- **crypto-group**
- **default terminal**
- **exit**
- **help**
- **logs checkpoint**
- **no logging active**
- **no logging trace**
- **no reveal disabled commands**
- **no timestamps**
- **no autoconfirm**
- **ping**

- **reveal disabled commands**
- **show** (except **show snmp communities** and **show snmp transports**)
- **sleep**
- **start crypto security-association**
- **terminal length**
- **terminal width**
- **timestamps**
- **traceroute**

Operator Mode Commands

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

- **aaa test**
- **alarm cutoff**
- **bulkstats force**
- **card**
- **clear** (a subset of all **clear** command variations)
- **debug**
- **dhcp test**
- **gtpc test**
- **gtpp interim**
- **gtpp test**
- **gtpu test**
- **gtpv0 test**
- **host**
- **logging active**
- **logging filter**
- **logging trace**
- **monitor protocol**
- **monitor subscriber**
- **newcall**
- **no card**
- **no debug**
- **no newcall policy**
- **port**
- **ppp echo-test**
- **radius interim accounting**
- **radius test**

- **rlogin**
- **show access-group**
- **show access-list**
- **show access-flow**
- **show access statistics**
- **show configuration**
- **show snmp transports**
- **ssh**
- **telnet**
- **test alarm**

Administrator Mode Commands

Administrators can access all system commands except:

- Context Configuration Mode:
  - **config-administrator**
  - **operator**
  - **inspector**
  - **administrator**
- Global Configuration Mode:
  - **snmp community**
  - **snmp user**
  - **local-user**
  - **suspend local-user**
- Exec Mode:
  - **show snmp communities**
  - **clear** (all **clear** command variations)
  - **show local-user**
  - **password change local-user**

Security Administrator Mode Commands

Security administrators can access all system commands.

CLI Contexts

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

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

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

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

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

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

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

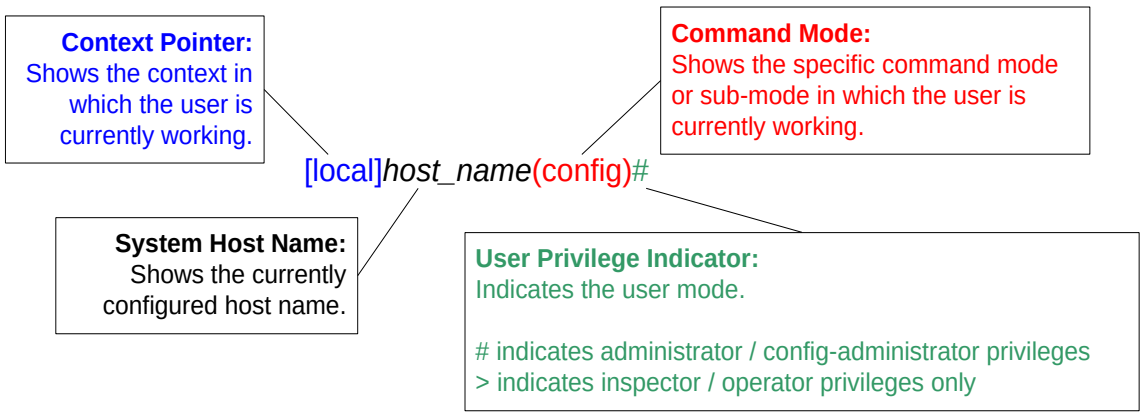
Understanding the CLI Command Prompt

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

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

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

Figure 2. CLI Command Prompt



CLI Command Syntax

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

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

Example

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

show port info *slot_number***/**

/*slot_number* is a variable representing a particular slot/ (1 through 48).

Entering and Viewing CLI Commands

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

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

Entering Partial CLI Commands

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

Example

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

```
Ambiguous Command
```

CLI Command Auto-completion

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

Example

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

[local]host_name# show
```

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

Example

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

show     shutdown

[local]host_name#
```

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

Example

```
[local]host_name# sh?

show - Displays information based on a specified argument

shutdown - Terminates execution of all tasks within the entire chassis
```

```
[local]host_name#
```

Using CLI Auto-Pagination

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

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

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

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

Using CLI Autoconfirmation

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

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

Example

Saving a configuration:

```
[local]host_name# save configuration

Are you sure ? [Yes | No]:
```

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

Examples

You create context named *newcontext*:

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

Are you sure ? [Yes | No]: yes

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

You revisit the context named "newcontext":

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

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

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

```
[local]host_name(config)# context mewcontext
```

```
Are you sure ? [Yes | No]:n

Action aborted

[local]host_name(config)#
```

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

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

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

You can control CLI autoconfirmation at the following levels:

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

Regulating the Command Output

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

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

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

Table 4. grep Keywords

Alternative Keyword	Description
-i	Specifies the filtering of the command's output for a particular expression while ignoring case. Lower case matches the same as upper case.
-v	Specifies the filtering of the command's output for everything excluding a particular expression.
--ignore-case	The long form of the **-i** option.
--invert-match	The long form of the **-v** option.
expression	Specifies the character pattern to find in the command's output.

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

Viewing Command History

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

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

Table 5. EMACS Shortcut Keystrokes

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

Obtaining CLI Help

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

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

Example

```
[local]host_name# test?

test - Performs test on followed mechanism
```

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

Example

```
[local]host_name# test alarm ?

audible - Tests internal audible alarm buzzer on SPC

central-office - Tests specified central office alarm relays on SPIO card

<cr> - newline
```

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

Example

```
[local]host_name# show card info ?

<Enter card number as an integer ranging 1 to 48> | - Pipeline <cr> -
Carriage Return or <Enter> key
```

Exiting the CLI and CLI Command Modes

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

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

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

Exiting Configuration Sub-modes

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

Example

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

[local]host_name(config)#
```

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

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

Example

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

[local]host_name#
```

Exiting Global Configuration Mode

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

Ending a CLI Session

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

Accessing the CLI

Access the CLI through the following methods:

- Local login through a Console port using the RS-232 serial cable supplied with the card
- Remote login using Telnet and Secure Shell (SSH) access to the CLI through any IP interface on the system. You can use remote login methods only after the system has been configured to support the various access methods.

Important: Even though you can access the CLI remotely through any available IP interface, it is recommended that management traffic be isolated from network traffic by using one of the SPIO card management interfaces.

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

Accessing the CLI Locally Using the Console Port

This section provides instructions for accessing the CLI locally through the console port on the SPIO.

Access the console port with the RJ-45-to-DB-9 serial (EIA-232) cable that is shipped with the Switch Processor Input/Output (SPIO) card. Connect to a workstation that has a communications application that accesses the workstation's serial port, such as Minicom for Linux or HyperTerminal® for MicroSoft Windows®.

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

For normal operation, the SMC in chassis slot 8 serves as the active processing card for the system. The SPIO that corresponds to this SMC is installed in slot 24. For the processing card in chassis slot 9, the corresponding SPIO is installed in slot 25.

Important: In the event of an SMC switchover, in which processes are switched from the card in slot 8 that was previously active to the redundant card in slot 9, the SPIO in slot 24 continues to serve as the active SPIO. Therefore, the console port is still accessible through that SPIO.

Follow the instructions below to connect to the console port.

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

Parameter	Setting
Baud Rate	115,200 bps
Data Bits	8

Parameter	Setting
Parity	None
Stop Bits	1
Flow Control	None

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

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

Remotely Accessing the CLI

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

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

IP Address Notation

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

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

IPv4 Dotted-Decimal Notation

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

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

IPv4 allows 32 bits for an Internet Protocol address and can, therefore, support 4,294,967,296 addresses

IPv6 Colon-Separated Notation

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

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

The hexadecimal digits are case-insensitive.

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

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

IPv6 allows 128 bits for an Internet Protocol address and can support 340,282,366,920,938,000,000,000,000,000,000,000,000,000 internet addresses.

CIDR Notation

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

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

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

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

For example:

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

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

Alphanumeric Strings

Some CLI commands require the entry of an alphanumeric string to define a value. The string is a contiguous collection of alphanumeric characters with a defined minimum and maximum length (number of characters).

Character Set

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

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

Do not use any of the following "special" characters in an alphanumeric string except as noted below:

- **&** (ampersand)
- **‘** (apostrophe)
- **< >** (arrow brackets) [see exception below]
- ***** (asterisk) [see wildcard exception below]
- **{ }** (braces)
- **[ ]** (brackets)
- **$** (dollar sign) [see wildcard exception below]
- **!** (exclamation point) [see exception below]
- **( )** [parentheses]
- **%** (percent) [see exception below]
- **#** (pound sign) [see exception below]
- **?** (question mark)
- **'** (quotation mark – single)
- **"** (quotation mark – double)
- **;** (semicolon)
- \ (slash – backward) [see exception below]
- / (slash – forward) [see exception below]
- ~ (tilde)
- | (vertical bar) [see exception below]

The following characters may appear in strings entered in ruledefs, APNs, license keys and other configuration/display parameters:

- **< >** (arrow brackets) [less than or greater than]
- ***** (asterisk) [wildcard]
- **:** (colon)
- **$** (dollar sign) [wildcard]

- **.** (dot)
- = (equals sign)
- **!** (exclamation point)
- **%** (percent)
- / (slash – forward)
- | (vertical bar)

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

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

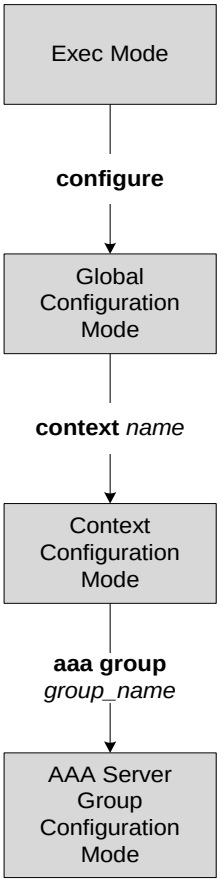
Quoted Strings

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

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

Chapter 2
AAA Server Group Configuration Mode Commands

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



diameter accounting

This command configures Diameter accounting parameters.

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

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

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

---

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

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

---

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

dictionary: Sets the context's dictionary as the system default.
hd-mode: Sends records to the Diameter server, if all Diameter servers are down or unreachable, then copies records to the local HDD and periodically retries the Diameter server.
max-retries: Sets the retry attempts for Diameter accounting in the current AAA group to default 0 (disable).
max-transmissions: Sets the configured maximum transmission attempts for Diameter accounting in the current AAA group to default 0 (disable).
request-timeout: Sets the timeout duration, in seconds, for Diameter accounting requests in the current AAA group to default 20.

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

Specifies the Diameter accounting dictionary.
aaa-custom1 ... aaa-custom10: Configures the custom dictionaries. Even though the CLI syntax supports several custom dictionaries, not necessarily all of them have been defined. If a custom dictionary that has not been implemented is selected, the default dictionary will be used.
nasreq: nasreq dictionary—the dictionary as defined by RFC 3588.
rf-plus: RF Plus dictionary.

endpoint *endpoint_name*

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

hd-mode fall-back-to-local

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

hd-storage-policy *hd_policy*

Associates the specified HD Storage policy with the AAA group.
hd_policy must be the name of a configured HD Storage policy, and must be an alphanumeric string of 1 through 63 characters.
HD Storage policies are configured through the Global Configuration Mode.
This and the **hd-mode** command are used to enable the storage of Rf Diameter Messages to HDD in case all Diameter Servers are down or unreachable.

max-retries *max_retries*

Specifies how many times a Diameter request should be retried with the same server, if the server fails to respond to a request.
max_retries specifies the maximum number of retry attempts, and must be an integer from 1 through 1000.
Default: 0

max-transmissions *max_transmissions*

Specifies the maximum number of transmission attempts for a Diameter request. Use this in conjunction with the **max-retries** *max_retries* option to control how many servers will be attempted to communicate with.
max_transmissions must be an integer from 1 through 1000.
Default: 0

request-timeout *request_timeout_duration*

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

server *host_name* **priority** *priority*

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

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

Usage

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

Example

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

```
diameter accounting dictionary aaa-custom10
```

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

```
diameter accounting endpoint EAP1
```

The following commands configure Diameter accounting options:

```
diameter accounting max-retries 4
```

```
diameter accounting max-transmissions 2
```

```
diameter accounting request-timeout 10
```

```
diameter accounting server svc priority 1
```

diameter authentication

This command configures Diameter authentication parameters.

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

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

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

---

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

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

---

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

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

dictionary { aaa-custom1 | aaa-custom10 | aaa-custom11 | aaa-custom12 | aaa-custom13 | aaa-custom14 | aaa-custom15 | aaa-custom16 | aaa-custom17 | aaa-custom18 | aaa-custom19 | aaa-custom2 | aaa-custom20 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 |aaa-custom8 | aaa-custom9 | nasreq }

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

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

aaa-custom9: Configures the STa standard dictionary.
nasreq: nasreq dictionary—the dictionary as defined by RFC 3588.

endpoint *endpoint_name*

Enables Diameter to be used for authentication, and specifies which Diameter endpoint to use.
endpoint_name must be an alphanumeric string of 1 through 63 characters.

max-retries *max_retries*

Specifies how many times a Diameter authentication request should be retried with the same server, if the server fails to respond to a request.
max_retries specifies the maximum number of retry attempts, and must be an integer from 1 through 1000.
Default: 0

max-transmissions *max_transmissions*

Specifies the maximum number of transmission attempts for a Diameter authentication request. Use this in conjunction with the "**max-retries** *max_retries*" option to control how many servers will be attempted to communicate with.
max_transmissions specifies the maximum number of transmission attempts, and must be an integer from 1 through 1000.
Default: 0

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

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

request-timeout *request_timeout_duration*

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

server *host_name* **priority** *priority*

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

Usage

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

Example

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

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

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

```
diameter authentication endpoint EAP1
```

The following commands configure Diameter authentication options:

```
diameter authentication max-retries 4

diameter authentication max-transmissions 2

diameter authentication redirect-host-avp primary-then-secondary

diameter authentication server svc priority 1

diameter authentication request-timeout 10
```

diameter authentication failure-handling

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

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

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

---

no

Disables Diameter authentication failure handling.

---

default

Configures the default Diameter authentication failure handling setting.

---

authorization-request

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

---

eap-request

Specifies configuring failure handling for EAP requests.

---

eap-termination-request

Specifies configuring failure handling for EAP termination requests.

---

request-timeout action { continue | retry-and-terminate | terminate }

Specifies the action to be taken for failures:

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

---

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

start_result_code: Specifies the result code number, must be an integer from 1 through 65535.

to *end_result_code*: Specifies the upper limit of a range of result codes. **to** *end_result_code* must be greater than *start_result_code*.

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

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

Usage

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

Example

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

```
diameter authentication failure-handling eap-request result-code 5001 to
5005 action continue

diameter authentication failure-handling eap-request result-code 5003
action terminate
```

diameter dictionary

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

end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

radius

This command configures basic RADIUS options.

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

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

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

no

Removes the specified configuration.

default

Configures default setting for the specified keyword.

dictionary *dictionary*

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

Dictionary	Description
custom*XX*	These are dictionaries that can be customized to fit your needs. Customization information can be attained by contacting your local service representative. *XX* is the integer value of the custom dictionary.
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.
3gpp	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in 3GPP 32.015.
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.

Dictionary	Description
starent-vsa1	This dictionary consists not only of the 3GPP2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary. ***Important:*** In 12.0 and later releases, no new attributes can be added to the **starent-vsa1** dictionary. If there are any new attributes to be added, these can only be added to the **starent** dictionary. For more information, please contact your Cisco account representative.
starent-vsa1-835	This dictionary consists not only of the 3gpp2-835 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary.
starent	This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.
starent-835	This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.

deadtime *minutes*

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

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

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

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

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

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

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

max-outstanding *max_messages*

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

max-retries *max_retries*

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

max-transmissions *max_transmissions*

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

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

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

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

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

timeout *idle_seconds*

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

Usage

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

Example

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

```
radius timeout 300
```

radius accounting

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

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

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

no

Removes the specified configuration.

default

Configures the default setting for the specified keyword.

archive [stop-only]

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

deadtime *minutes*

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

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

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

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

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

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

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

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

fire-and-forget

Enables RADIUS Fire-and-Forget accounting for the AAA group.
Default: Disabled
The request sent to the RADIUS accounting server configured under the AAA group with this keyword configured will not expect a response from the server. If the request must be sent to more than one such type of server, the acct-algorithm first-n configuration in the AAA group can be used.
Keepalive feature for server state detection is supported in conjunction since there is no waiting for responses. Archiving in such a AAA group is not supported. If the server is down, the request is sent to the next server in the group. If all the servers in the group are down, the request is deleted.
This CLI is independent of the APN or subscriber profile configuration **aaa secondary-group** *aaa_group_name*.

interim interval *interim_interval*

Specifies the time interval, in seconds, for sending accounting INTERIM-UPDATE records.
interim_interval must be an integer from 50 through 40000000.
Default: Disabled

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

max-outstanding *max_messages*

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

max-pdu-size *octets*

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

max-retries *max_retries*

Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as "Not Responding" and the detect dead server consecutive failures count is incremented.
max_retries must be an integer from 0 through 65535.
Default: 5
Once the maximum number of retries is reached this is considered a single failure for the consecutive failures count for detecting dead servers.

max-transmissions *max_transmissions*

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

timeout *timeout_duration*

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

Usage

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

Example

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

```
radius accounting timeout 16
```

radius accounting apn-to-be-included

This command specifies the APN name inclusion for RADIUS accounting.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

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

default radius accounting apn-to-be-included
```

default

Configures the default setting.

gi

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

gn

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

Usage

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

Example

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

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

radius accounting algorithm

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

default radius accounting algorithm

default

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

first-n *n*

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

first-server

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

round-robin

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

Usage

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

Example

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

```
radius accounting algorithm round-robin
```

radius accounting billing-version

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius accounting billing-version *version*

default radius accounting billing-version

default

Configures the default setting.
Default: 0

version

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

Usage

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

Example

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

```
radius accounting billing-version 10
```

radius accounting gtp trigger-policy

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

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

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

default radius accounting gtp trigger-policy
```

default

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

standard

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

ggsn-preservation-mode

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

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

Usage

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

Example

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

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

radius accounting ha policy

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

Product

HA

Privilege

Security Administrator, Administrator

Syntax

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

default radius accounting ha policy
```

default

Configures the default setting.

session-start-stop

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

custom1-aaa-res-mgmt

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

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

Usage

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

Example

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

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

radius accounting interim

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

Product

GGSN, PDSN, HA, HSGW

Privilege

Security Administrator, Administrator

Syntax

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

no radius accounting interim volume

no

Disables RADIUS interim accounting.

interval *interim_interval*

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

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

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

Usage

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

Example

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

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

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

```
radius accounting interim interval 180
```

radius accounting ip remote-address

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

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

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

`no`

Removes the specified configuration.

`collection`

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

`list` *`list_id`*

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

Usage

This command is used as part of the Remote Address-based Accounting feature to both configure remote IP address lists and enable the collection of accounting data for the addresses in those lists on a per-subscriber basis.
Individual subscriber can be associated to remote IP address lists through the configuration/specification of an attribute in their local or RADIUS profile. (Refer to the **`radius accounting`** command in the Subscriber Configuration mode.) When configured/specified, accounting data is collected pertaining to the subscriber's communication with any of the remote addresses specified in the list.
Once this functionality is configured on the system and in the subscriber profiles, it must be enabled by executing this command with the collection keyword.

Example

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

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

radius accounting keepalive

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

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

no radius accounting keepalive framed-ip-address

no

Removes the specified configuration.

default

Configures the default setting for the specified keyword.

calling-station-id *id*

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

consecutive-response *consecutive_responses*

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

framed-ip-address *ip_address*

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

interval *seconds*

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

retries *number*

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

Default: 3

timeout *timeout_duration*

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

username *user_name*

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

Usage

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

Example

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

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

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

```
radius accounting keepalive retries 4
```

radius accounting pdif trigger-policy

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

Product

PDIF

Privilege

Administrator, Security Administrator

Syntax

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

default radius accounting pdif trigger-policy
```

default

The default option configures the “standard” policy.

standard

Applies a policy as defined by the standards.

counter-rollover

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

Usage

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

Example

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

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

radius accounting rp

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

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

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

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

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

---

no

Removes the specified configuration.

---

default

Sets the default configuration for the specified keyword.

---

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

Specifies the behavior of generating accounting STOP when handoff occurs.

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

Default: **wait-active-stop**

---

tod *minute hour*

Specifies the time of day a RADIUS event is to be generated for accounting. Up to four different times of the day may be specified through individual commands.
minute must be an integer from 0 through 59.
hour must be an integer from 0 through 23.

---

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

active-start-param-change: Enabled
active-stop: Disabled
Configures the events for which a RADIUS event is generated for accounting as one of the following:

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

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

Default: **active-handoff**: Disabled

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

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

Default: **airlink-usage**: Disabled
custom:
active-handoff = Disabled
active-start-param-change = Disabled
active-stop = Disabled
standard: Enabled
Configures the overall accounting policy for R-P sessions as one of the following:

- **airlink-usage [counter-rollover]**: Specifies the use of Airlink-Usage RADIUS accounting policy for R-P, which generates a start on Active-Starts, and a stop on Active-Stops.
- If the **counter-rollover** option is enabled, the system generates a STOP/START pair before input/output data octet counts (or input/output data packet counts) become larger than (2^32 - 1) in value. This setting is used to guarantee that a 32-bit octet count in any STOP message has not wrapped to larger than 2^32 thus ensuring the accuracy of the count. The system, may, at its discretion, send the STOP/START pair at any time, so long as it does so before the 32-bit counter has wrapped. Note that a STOP/START pair is never generated unless the subscriber RP session is in the Active state, since octet/packet counts are not accumulated when in the Dormant state.
- **custom**: Specifies the use of custom RADIUS accounting policy for R-P. The custom policy can consist of the following:
- **active-handoff**: Enables a single R-P event (and therefore a RADIUS accounting event) when an Active PCF-to-PFC Handoff occurs. Normally two R-P events will occur (one for the Connection Setup, and the second for the Active-Start)
- **active-start-param-change**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Start is received from the PCF and there has been a parameter change.

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

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

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

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

trigger-stop-start

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

Usage

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

Example

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

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

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

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

radius accounting server

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

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

no

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

mediation-device

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

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

ip_address **[port** *port_number* **]**

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

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

[encrypted] key *value*

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

key keyword is the encrypted version of the plaint text key. Only the encrypted key is saved as part of the configuration file.

---

acct-on { disable | enable }

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

---

acct-off { disable | enable }

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

---

max *max_messages*

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

---

max-rate *max_value*

Specifies the rate at which the accounting messages should be sent to the RADIUS server by a single AAA manager task.
max_value must be an integer from 0 through 1000.
Default: 0 (disabled)

---

oldports

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

---

priority *priority*

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

type { mediation-device | standard }

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

admin-status { disable | enable }

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

-noconfirm

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

Usage

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

Example

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

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

radius algorithm

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

default radius algorithm
```

default

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

first-server

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

round-robin

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

Usage

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

Example

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

```
radius algorithm round-robin
```

radius allow

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

Product

All products used in CDMA deployments

Privilege

Security Administrator, Administrator

Syntax

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

no

Specifies that the specified option is to be disabled.

authentication-down

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

accounting-down

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

Usage

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

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

Example

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

```
radius allow accounting-down
```

radius attribute

This command configures the system's RADIUS identification parameters.

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

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

default radius attribute nas-identifier
```

no

Removes the specified configuration.

default

Configures the default setting.

nas-identifier *nas_id*

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

nas-ip-address address *primary_address*

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

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

backup *secondary_address*

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

nexthop-forwarding-address *nexthop_address*

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

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

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

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

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

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

vlan *vlan_id*

This optional keyword sets the RADIUS client to provide VLAN ID with nexthop forwarding address to system when running in single nexthop gateway mode.
vlan_id must be a pre-configured VLAN ID, and must be an integer from 1 through 4096. It is the VLAN ID to be provided to the system in RADIUS attributes.
This option is available only when nexthop-forwarding gateway is also configured with nexthop-forwarding-address *nexthop_address* keyword and **aaa-large configuration** is enabled at Global Configuration level.

Usage

This is necessary for NetWare Access Server usage such as the system must be identified to the NAS.
The system supports the concept of the active nas-ip-address. The active nas-ip-address is defined as the current source ip address for RADIUS messages being used by the system. This is the content of the nas-ip-address attribute in each RADIUS message.
The system will always have exactly one active nas-ip-address. The active nas-ip-address will start as the primary nas-ip-address. However, the active nas-ip-address may switch from the primary to the backup, or the backup to the primary. The following events will occur when the active nas-ip-address is switched:

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

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

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

Example

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

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

radius authenticate

This command configures RADIUS authentication related parameters.

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

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

no radius authenticate null-username
```

default

Configures the default setting.

no radius authenticate null-username

Disables sending an Access-Request message to the AAA server for user names (NAI) that are blank.

apn-to-be-included

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

null-username

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

Usage

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

Example

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

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

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

```
radius authenticate null-username
```

radius authenticator-validation

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

no

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

Usage

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

Example

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

```
no radius authenticator-validation
```

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

```
radius authenticator-validation
```

radius charging

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

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

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

---

no

Removes the specified configuration.

---

default

Configures the default setting for the specified keyword.

---

deadtime *dead_time*

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

---

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

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

---

max-outstanding *max_messages*

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

max-retries *max_retries*

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

max-transmissions *max_transmissions*

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

timeout *idle_seconds*

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

Usage

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

Example

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

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

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

```
radius charging timeout 300
```

radius charging accounting algorithm

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

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

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

first-n *n*

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

first-server

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

round-robin

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

Usage

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

Example

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

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

radius charging accounting server

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

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

---

no

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

---

ip_address

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

[encrypted] key *value*

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

---

max *max_messages*

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

---

oldports

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

---

port *port_number*

Specifies the port number to use for communication.

port_number must be an integer from 0 through 65535.
Default: 1813

priority *priority*

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

admin-status { enable | disable }

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

-noconfirm

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

Usage

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

Example

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

```
radius charging accounting server 10.1.2.3 key sharedKey212 port 1024 max
127

radius charging accounting server 10.1.2.3 encrypted key scrambledKey234
oldports priority 10
```

radius charging algorithm

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

default radius charging algorithm
```

default

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

first-server

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

round-robin

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

Usage

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

Example

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

```
radius algorithm round-robin
```

radius charging server

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

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

---

no

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

---

ip_address

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

[encrypted] key *value*

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

---

max *max_messages*

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

---

oldports

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

---

port *port_number*

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

Default: 1812

priority *priority*

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

admin-status { enable | disable }

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

-noconfirm

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

Usage

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

Example

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

```
radius charging server 10.2.3.4 key sharedKey212 port 1024 max 127

radius charging server 10.2.3.4 encrypted key scrambledKey234 oldports
priority 10
```

radius ip vrf

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius ip vrf *vrf_name*

no radius ip vrf

no

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

vrf_name

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

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

Usage

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

Example

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

```
radius ip vrf ip_vrf1
```

radius keepalive

This command configures the RADIUS keepalive authentication parameters.

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

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

default

Configures the default setting for the specified keyword.

calling-station-id *id*

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

consecutive-response *number*

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

encrypted password

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

interval *seconds*

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

password

Specifies the password to be used for authentication.
password must be an alphanumeric string of 1 through 63 characters.
Default password: Test-Password

retries *number*

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

timeout *timeout_duration*

Specifies the time interval between keepalive access request retries.
timeout_duration must be an integer from 1 through 30.
Default: 3 seconds

username *user_name*

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

valid-response access-accept [*access-reject* **]**

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

Usage

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

Example

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

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

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

```
radius keepalive retries 4
```

radius mediation-device

See the radius accounting server command.

radius probe-interval

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius probe-interval *seconds*

default radius probe-interval

default

Configures the default setting.

seconds

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

Usage

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

Example

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

```
radius probe-interval 30
```

radius probe-max-retries

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius probe-max-retries *retries*

default radius probe-max-retries

default

Configures the default setting.

retries

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

Usage

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

Example

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

```
radius probe-max-retries 6
```

radius probe-timeout

This command configures the timeout duration for Interchassis Session Recovery (ICSR) to wait for a response for RADIUS authentication probes.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius probe-timeout *idle_seconds*

default radius probe-timeout

default

Configures the default setting.

idle_seconds

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

Usage

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

Example

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

```
radius probe-timeout 120
```

radius server

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

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

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

no

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

ip_address **port** *port_number*

Specifies the IP address and port number of the server.
ip_address: Must be specified using IPv4 dotted-decimal notation. A maximum of 1600 RADIUS servers per context/system and 128 servers per Server group can be configured. This limit includes accounting and authentication servers.
port *port_number*: Specifies the port number to use for communications. *port_number* must be an integer from 1 through 65535.
Default: 1812.

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

[encrypted] key *value*

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

admin-status { disable | enable }

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

max *max_messages*

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

max-rate *max_value*

Specifies the rate at which the authentication messages should be sent to the RADIUS server by a single AAA manager task.
max_value must be an integer from 0 through 1000.
Default: 0 (disabled)

oldports

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

priority *priority*

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

probe

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

no-probe

Disable probe messages from being sent to the specified RADIUS server. This is the default behavior.

probe-username *user_name*

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

probe-password [encrypted] password *password*

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

type { mediation-device | standard }

Specifies the type of transactions the RADIUS server accepts.
mediation-device: Specifies mediation-device specific AAA transactions. This device is available if you purchased a transaction control services license. Contact your local Cisco representative for licensing information.

standard: Specifies standard AAA transactions. (Default)

-noconfirm

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

Usage

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

Example

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

```
radius server 10.2.3.4 key sharedKey212 port 1024 max 127

radius server 10.2.3.4 encrypted key scrambledKey234 oldports priority 10
```

radius trigger

This command enables specific RADIUS triggers.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

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

default radius trigger
```

no

Disables specified RADIUS trigger.

default

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

ms-timezone-change

Specifies to enable RADIUS trigger for MS time zone change.

qos-change

Specifies to enable RADIUS trigger for Quality of Service change.

rai-change

Specifies to enable RADIUS trigger for Routing Area Information change.

rat-change

Specifies to enable RADIUS trigger for Radio Access Technology change.

serving-node-change

Specifies to enable RADIUS trigger for Serving Node change.

uli-change

Specifies to enable RADIUS trigger for User Location Information change.

Usage

Use this command to enable RADIUS triggers.

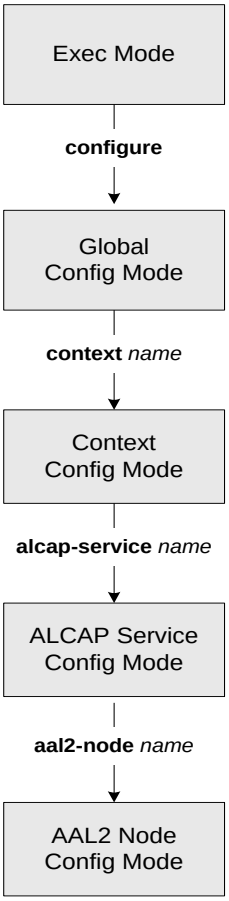
Example

The following command enables RADIUS trigger for RAT change:

```
radius trigger rat-change
```

Chapter 3
AAL2 Node Configuration Mode Commands

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



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

aal2-path-id

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

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

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

no

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

aal2_path_id

Specifies the AAL2 path identifier configured with adjacent AAL2 node(s). The AAL2 path id must be unique within an AAL2 node configuration. This value is used to identify a particular path towards an adjacent AAL2 node and is sent in ALCAP protocol messages to peer where path identification is required. The *aal2_path_id* must be an integer between 1 through 4294967295.

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

block

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

Usage

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

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

Example

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

```
al2-path-id 2
```

Following command unblocks the AAL2 path identifier *6* which was earlier blocked in an AAL2 node configuration.

no al2-path-id *6* **block**

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Return to the previous mode.

point-code

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

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

[no] point-code *point_code*

no

Removes the configured point code from this AAL2 node configuration.

point_code

Defines the point code to assign to adjacent AAL2 node in SS7 format.
point_code: value entered must adhere to the point code variant selected when the AAL2 node was defined:

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- a string of 1 to 11 combined digits ad period.

Usage

Use this command to configure configure the point code of adjacent AAL2 node in SS7 format address. This point code shall be filled in the destination point-code (dpc) field of MTP3 routing label. This is required if signaling transport network is based on MTP3-broadband (MTP3B).
A maximum of 16 point codes for adjacent AAL2 nodes can be configured in one ALCAP service.

Example

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

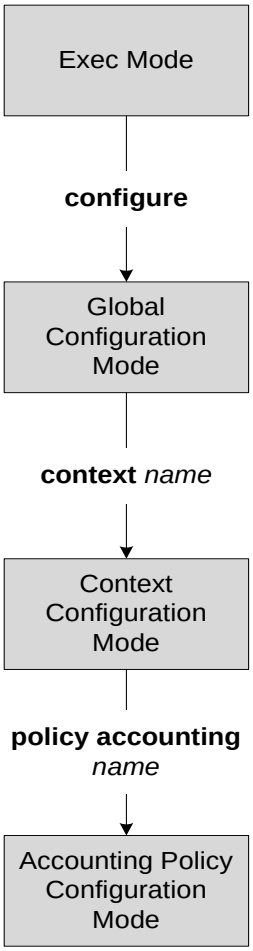
```
point-code 4.121.5
```

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

```
no point-code 4.121.15
```

Chapter 4
Accounting Policy Configuration Mode Commands

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



accounting-event-trigger

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

Product

HSGW, P-GW, S-GW

Privilege

Administrator

Syntax

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

[ default | no ] accounting-event-trigger { cgi-sai-change | ecgi-change | flow-
information-change | interim-timeout | location-change | rai-change | tai-change }
```

default

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

no

Removes the specified event trigger configuration from this policy.

cgi-sai-change

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

ecgi-change

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

flow-information-change

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

interim-timeout

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

location-change

Specifies that the action is initiated upon indication of a location change.

rai-change

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

tai-change

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

action { interim | stop-start }

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

Usage

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

Example

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

```
accounting-event-trigger interim-timeout action stop-start
```

accounting-keys

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

Product

HSGW, P-GW, S-GW

Privilege

Administrator

Syntax

```
accounting-keys qci

default accounting-keys
```

default

Aggregate the accounting information, using QoS Class Identifier (QCI) as the additional key.

qci

Aggregate the accounting information, using QCI as the additional key.

Usage

Use this command to aggregate the accounting information, using the configurable keys (QCI) along with default keys.
In service data flow (SDF) level accounting, buckets are created and maintained using the Reporting-Level AVP value present in Gx message. The following are the accounting keys currently supported:

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

Example

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

```
accounting-keys qci
```

accounting-level

Configures the type of accounting performed by this profile.

Product

HSGW, P-GW, S-GW

Privilege

Administrator

Syntax

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

default accounting-level
```

default

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

flow

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

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

pdn

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

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

pdn-qci

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

- Addresses allocated to the UE in this PDN

- PDN identifier
- QCI for which accounting is done
- User Equipment information if available (ESN/MEID)
- Address of HSGW/S-GW
- Address of the P-GW (if available), one or more instances

qci

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

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

sdf

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

subscriber

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

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

Usage

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

Example

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

```
accounting-level flow
```

accounting-mode

Configures the accounting mode for this profile.

Product

HSGW, P-GW, S-GW

Privilege

Administrator

Syntax

```
accounting-mode normal

default accounting-mode
```

default

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

normal

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

Usage

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

cc

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

Product

S-GW, HSGW, P-GW

Privilege

Administrator

Syntax

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

default cc profile index

no cc profile index { buckets | interval | sdf-interval | sdf-volume | serving-nodes |
tariff | volume }
```

default

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

no

Returns the specified feature to its default setting.

profile *index*

Specifies a billing type to be applied to this profile. *index* must be one of the following:
1: Hot billing
2: Flat billing
4: Prepaid billing
8: Normal billing

buckets *num*

Default: 4
Specifies the number of container changes in the S-GW CDR due to QoS changes or tariff times. If an accounting policy is not configured, this value is 4. GTPP accounting will use the default value if the configured value is beyond 4.
In 12.0 and earlier releases, *num* must be an integer value from 1 through 4.
In 12.2 and later releases, *num* must be an integer value from 1 through 10.

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

interval *seconds*

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

sdf-interval *seconds*

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

sdf-volume { downlink *octets* **{ uplink** *octets* **} | total** *octets* **| uplink** *octets* **{ downlink** *octets* **} }**

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

serving-nodes *num*

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

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

Specifies time-of-day values used to determine when a container is closed in the charging records.
time1 *min hrs*: Specifies the first time-of-day value used to close the current container in the charging record. *min* must be an integer value from 0 through 59. *hrs* must be an integer value from 0 through 23.
time2 *min hrs*...**time4** *minutes hours*: Specifies the second, third and fourth time-of-day values used to close containers in the charging record. *min* must be an integer value from 0 through 59. *hrs* must be an integer value from 0 through 23.

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

Specifies octet volume thresholds for the generation of interim CDRs.
downlink *octets*: Sets the threshold limit for the number of downlink octets that must be reached before the charging record is closed.
In 12.1 and earlier releases, the downlink *octets* must be an integer value from 100000 to 1345294336.
In 12.2 and later releases, the downlink *octets* must be an integer value from 100000 to 4000000000.
total *octets*: Sets the threshold limit for the total number of octets that must be reached before the charging record is closed.
In 12.1 and earlier releases, the total*octets* must be an integer value from 100000 to 400000000.
In 12.2 and later releases, the total *octets* must be an integer value from 100000 to 4000000000.

uplink *octets*: Sets the threshold limit for the number of uplink octets that must be reached before the charging record is closed.
In 12.1 and earlier releases, the uplink *octets* must be an integer value from 100000 to 400000000.
In 12.2 and later releases, the uplink *octets* must be an integer value from 100000 to 4000000000.

Usage

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

Example

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

```
cc profile 1 volume total 500000
```

end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

max-containers

Control the number of containers in an ACR message.

Product

GGSN, HSGW, P-GW, S-GW

Privilege

Administrator

Syntax

max-containers { *containers* | fill-buffer }

default max-containers

default

Cache containers until buffer is filled.

containers

System can send any value equal or less than the maximum number of containers selected. The number of containers that can be sent can be dynamically selected by the system, but it should not cross the limit of containers in any message.
containers must be in integer from 1 to 30.

fill-buffer

Cache containers until buffer is filled.

Usage

Use this command to control the number of containers before an interim ACR message is triggered.

Example

The following command sets a maximum of *20* containers in an ACR message:

```
max-containers 20
```

operator-string

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

Product

HSGW, P-GW, S-GW

Privilege

Administrator

Syntax

operator-string *string*

no operator-string

no

Removes the operator string from this policy.

string

Specifies a text string that is included with accounting messages originating from this policy. *string* must be from 1 to 63 alphanumeric characters.

Usage

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

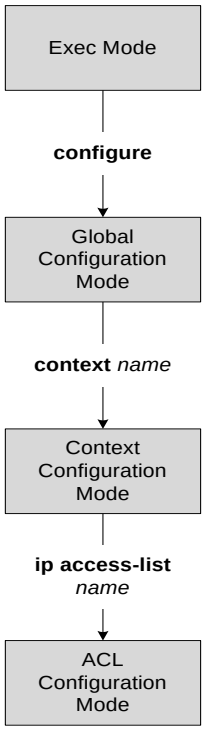
Example

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

```
operator-string pgw_local
```

Chapter 5
ACL Configuration Mode Commands

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



deny/permit (by source IP address masking)

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
{ deny | permit } [ log ] source_address source_wildcard

after { deny | permit } [ log ] source_address source_wildcard

before { deny | permit } [ log ] source_address source_wildcard

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

after

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

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

before

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

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

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

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

source_address

The IP address(es) from which the packet originated. IP addresses must be entered in IPv4 dotted-decimal format.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

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

Usage

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

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

Example

The following command defines two rules with the second logging filtered packets:

```
permit 1.2.3.0 0.0.0.31

deny log 1.2.4.0 0.0.0.15
```

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

```
before permit 1.2.3.0 0.0.0.31
```

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

```
after deny log 1.2.4.0 0.0.0.15
```

The following deletes the first rule defined above:

```
no permit 1.2.3.0 0.0.0.31
```

deny/permit (any)

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
{ deny | permit } [ log ] any

after { deny | permit } [ log ] any

before { deny | permit } [ log ] any

no { deny | permit } [ log ] any
```

after

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

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

before

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

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

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: Packets are not logged.

Indicates all packets which match the filter are to be logged.

any

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

Usage

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

Important: It is suggested that any rule which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

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

```
permit any

deny log any
```

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

```
before permit any
```

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

```
after deny log any
```

The following deletes the first rule defined above:

```
no permit any
```

deny/permit (by host IP address)

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

{ deny | permit } [log] host *source_host_address*

after { deny | permit } [log] host *source_host_address*

before { deny | permit } [log] host *source_host_address*

no { deny | permit } [log] host *source_host_address*

after

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

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

before

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

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

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: Packets are not logged.
Indicates that all packets which match the filter are to be logged.

source_host_address

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

Usage

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

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

Example

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

```
permit host 10.2.3.4

deny log host 10.2.3.5
```

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

```
before permit host 10.2.3.4
```

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

```
after deny log host 10.2.3.5
```

The following deletes the first rule defined above:

```
no permit host 10.2.3.4
```

deny/permit (by source ICMP packets)

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
{ deny | permit } [ log ] icmp { source_address source_wildcard | any | host
source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [
icmp_type [ icmp_code ] ]

after { deny | permit } [ log ] icmp { source_address source_wildcard | any | host
source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [
icmp_type [ icmp_code ] ]

before { deny | permit } [ log ] icmp { source_address source_wildcard | any | host
source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [
icmp_type [ icmp_code ] ]

no { deny | permit } [ log ] icmp { source_address source_wildcard | any | host
source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [
icmp_type [ icmp_code ] ]
```

after

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

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

before

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

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

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

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

source_address

The IP address(es) from which the packet originated. IP addresses must be entered in IPv4 dotted-decimal format.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

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

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

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

dest_host_address

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

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

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

icmp_type

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

icmp_code

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

Usage

Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk. The IP filtering allows flexible controls for pairs of individual hosts or groups by IP masking which allows the filtering of entire subnets if necessary.

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

Example

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

```
permit icmp host 10.2.3.4 any 168

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

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

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

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

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

The following deletes the first rule defined above:

```
no permit icmp host 10.2.3.4 any 168
```

deny/permit (by IP packets)

Filters subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
{ deny | permit } [ log ] ip { source_address source_wildcard | any | host
source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [
fragment ] [ protocol num ]

after { deny | permit } [ log ] ip { source_address source_wildcard | any | host
source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [
fragment ] [ protocol num ]

before { deny | permit } [ log ] ip { source_address source_wildcard | any | host
source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [
fragment ] [ protocol num ]

no { deny | permit } [ log ] ip { source_address source_wildcard | any | host
source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [
fragment ] [ protocol num ]
```

after

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

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

before

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

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

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

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

source_address

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

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

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

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

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

dest_host_address

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

dest_address

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

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

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

fragment

Indicates packet filtering is to be applied to IP packet fragments only.

protocol *num*

Indicates that the packet filtering is to be applied to a specific protocol number.
num can be an integer ranging from 0 to 255.

Important: This keyword is not applicable to a SPIO interface. Instead, you must specify the type of protocol packets for which you want to deny/permit processing on a SPIO. For example, **deny icmp**, **deny tcp**, or **deny udp**.

Usage

Block IP packets when the source and destination are of interest.

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

Example

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

```
permit ip host 10.2.3.4 any fragment

deny log ip 10.2.3.0 0.0.0.31 host 10.2.4.16
```

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

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

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

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

The following deletes the first rule defined above:

```
no permit ip host 10.2.3.4 any fragment
```

deny/permit (by TCP/UDP packets)

Filters subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
{ deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard | any | host
source_host_address } [ eq source_port | gt source_port | lt source_port | neq
source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq
dest_port | gt dest_port | lt dest_port | neq dest_port | range start_port end_port ] }

after { deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard | any |
host source_host_address } [ eq source_port | gt source_port | lt source_port | neq
source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq
dest_port | gt dest_port | lt dest_port | neq dest_port | range start_port end_port ] }

before { deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard | any |
host source_host_address } [ eq source_port | gt source_port | lt source_port | neq
source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq
dest_port | gt dest_port | lt dest_port | neq dest_port | range start_port end_port ] }

no { deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard | any |
host source_host_address } [ eq source_port | gt source_port | lt source_port | neq
source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq
dest_port | gt dest_port | lt dest_port | neq dest_port | range start_port end_port ] }
```

after

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

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

before

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

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

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

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

tcp | udp

Specifies the filter is to be applied to IP based transmission control protocol or the user datagram protocol.

- **tcp**: Filter applies to TPC packets.
- **udp**: Filter applies to UDP packets.

source_address

The IP address(es) from which the packet originated. IP addresses must be entered in IPv4 dotted-decimal format.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

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

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

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

dest_host_address

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

eq *source_port*

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

gt *source_port*

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

lt *source_port*

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

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be an integer from 0 through 65535.

dest_address

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

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

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

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be an integer from 0 through 65535.

gt *dest_port*

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

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.
dest_port must be an integer from 0 through 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.
dest_port must be an integer from 0 through 65535.

range *start_port end_port*

Specifies a range of ports to be matched.
start_port must be an integer from 0 through 65535, and must be less than the *end_port* value.
end_port must be an integer from 0 through 65535, and must be greater than the *start_port* value.

Important: This option is supported in PDIF Release 8.3.

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

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

Example

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

```
permit tcp host 10.2.3.4 any

deny log udp 10.2.3.0 0.0.0.31 host 10.2.4.16

permit tcp host 10.2.3.64 gt 1023 any

deny log udp 10.2.3.0 0.0.0.31 10.2.4.127 0.0.0.127
```

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

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

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

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

The following deletes the third rule defined above:

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

end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

readdress server

Alters the destination address and port number in TCP or UDP packet headers to redirect packets to a different server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

readdress server *redirect_address* **[port** *port_no* **] { tcp | udp } { { source_address** *source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { { dest_address dest_wildcard | any | host** *dest_host_address* **} [eq]** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **] }**

after readdress server *redirect_address* **[port** *port_no* **] { tcp | udp } { { source_address** *source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { { dest_address dest_wildcard | any | host** *dest_host_address* **} [eq]** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **] }**

before readdress server *redirect_address* **[port** *port_no* **] { tcp | udp } { { source_address** *source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { { dest_address dest_wildcard | any | host** *dest_host_address* **} [eq]** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **] }**

no readdress server *redirect_address* **[port** *port_no* **] { tcp | udp } { { source_address** *source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { { dest_address dest_wildcard | any | host** *dest_host_address* **} [eq]** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **] }**

after

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

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

before

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

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

no

Removes the rule which exactly matches the options specified.

redirect_address

The IP address to which the IP packets are redirected. TCP or UDP packet headers are rewritten to contain the new destination address. This must be an IPv4 address specified in dotted-decimal notation.

port *port_no*

The number of the port at the redirect address where the packets are sent. TCP or UDP packet headers are rewritten to contain the new destination port number.

tcp | udp

Specifies the redirect is to be applied to the IP based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TCP packets.
- **udp**: Redirect applies to UDP packets.

source_address

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

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

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

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

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

dest_host_address

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

eq *source_port*

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

gt *source_port*

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

lt *source_port*

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

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be an integer from 0 through 65535.

dest_address

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

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

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

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be an integer from 0 through 65535.

gt *dest_port*

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

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered. *dest_port* must be an integer 0 through 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. *dest_port* must be an integer 0 through 65535.

Usage

Use this command to define a rule that redirects packets to a different destination address. The TCP and UDP packet headers are modified with the new destination address and destination port.

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

Important: Prior to Release 8.3, for packets received from the packet data network destined for a subscriber's UE, the system applied logic to reset the source address of a packet to the original destination address of the input packet before applying the outbound access control list (ACL). In Release 8.3 and higher, the system reverses the order and applies the outbound ACL before resetting the source address. This change impacts all current readdress server rules in inbound IPv4 ACLs.

Important: After Release 8.3, for every readdress server rule in an inbound IPv4 ACL, you must add a permit rule to an outbound ACL that explicitly permits packets from the readdress rule's redirect address and port number. If the permit rule is omitted, the system will reject all packets destined for the subscriber's UE from the readdress rule's redirect address and port number.

Example

The following command defines a rule that redirects packets to the server at 192.168.10.4, UDP packets coming from any host with a destination of any host are matched:

```
readdress server 192.168.10.4 udp any any
```

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

```
before readdress server 192.168.10.4 udp any any
```

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

```
after readdress server 192.168.10.4 udp any any
```

The following deletes the rule defined above:

```
no readdress server 192.168.10.4 udp any any
```

redirect context (by IP address masking)

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect context *context_id* **[log]** *source_address source_wildcard*

after redirect context *context_id* **[log]** *source_address source_wildcard*

before redirect context *context_id* **[log]** *source_address source_wildcard*

no redirect context *context_id* **[log]** *source_address source_wildcard*

after

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

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

before

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

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

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

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

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

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

Usage

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

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

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

Example

The following command defines a rule that redirects packets to the context with the context ID of 23 and the source IP and wildcard of 192.168.22.0 and 0.0.0.31:

```
redirect context 23 198.162.22.0 0.0.0.31
```

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

```
before redirect context 23 198.162.22.0 0.0.0.31
```

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

```
after redirect context 23 198.162.22.0 0.0.0.31
```

The following deletes the first rule defined above:

```
no redirect context 23 198.162.22.0 0.0.0.31
```

redirect context (any)

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect context *context_id* **[log] any**

after redirect context *context_id* **[log] any**

before redirect context *context_id* **[log] any**

no redirect context *context_id* **[log] any**

after

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

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

before

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

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

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any

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

Usage

Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

Important: Any rule which is added as a catch all should also have the log option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security.

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

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

Example

The following command defines a rule that redirects packets to the context with the context ID of 23 and any source IP:

```
redirect context 23 any
```

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

```
before redirect context 23 any
```

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

```
after redirect context 23 any
```

The following deletes the first rule defined above:

```
no redirect context 23 any
```

redirect context (by host IP address)

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

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect context *context_id* **[log] host** *source_ipv4_address*

after redirect context *context_id* **[log] host** *source_ipv4_address*

before redirect context *context_id* **[log] host** *source_ipv4_address*

no redirect context *context_id* **[log] host** *source_ipv4_address*

after

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

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

before

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

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

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_ipv4_address

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

Usage

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

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

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

Example

The following command defines a rule that redirects packets to the context with the context ID of 23 and a host IP address of 192.168.200.11:

```
redirect context 23 host 192.168.200.11
```

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

```
before redirect context 23 host 192.168.200.11
```

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

```
after redirect context 23 host 192.168.200.11
```

The following deletes the first rule defined above:

```
no redirect context 23 host 192.168.200.11
```

redirect context (by source ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect context *context_id* **[log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

after redirect context *context_id* **[log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

before redirect context *context_id* **[log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

no redirect context *context_id* **[log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

after

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

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

before

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

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

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

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

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

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

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

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

dest_host_address

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

dest_address

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

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

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

icmp_type

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

icmp_code

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

Usage

Define a rule to block ICMP packets which can be used for address resolution and possibly be a security risk. The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

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

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

Example

The following command defines a rule that redirects packets to the context with the context ID of 23, and ICMP packets coming from the host with the IP address 198.162.100.25:

```
redirect context 23 icmp host 192.168.100.25
```

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

```
before redirect context 23 icmp host 192.168.100.25
```

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

```
after redirect context 23 icmp host 192.168.100.25
```

The following deletes the first rule defined above:

```
no redirect context 23 icmp host 192.168.100.25
```

redirect context (by IP packets)

Redirects subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect context *context_id* **[log] ip { *source_address source_wildcard* | **any** | **host** *source_host_address* } { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**fragment**] [**protocol** *num*]**

after redirect context *context_id* **[log] ip { *source_address source_wildcard* | **any** | **host** *source_host_address* } { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**fragment**] [**protocol** *num*]**

before redirect context *context_id* **[log] ip { *source_address source_wildcard* | **any** | **host** *source_host_address* } { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**fragment**] [**protocol** *num*]**

no redirect context *context_id* **[log] ip { *source_address source_wildcard* | **any** | **host** *source_host_address* } { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**fragment**] [**protocol** *num*]**

after

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

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

before

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

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

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

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

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

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

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

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

dest_host_address

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

dest_address

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

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

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

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

protocol *num*

Indicates that the packet filtering is to be applied to a specific protocol number.
num can be an integer ranging from 0 to 255.

Usage

Block IP packets when the source and destination are of interest.

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

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

Example

The following command defines a rule that redirects packets to the context with the context ID of 23, and IP packets coming from the host with the IP address 198.162.100.25, and fragmented packets for any destination are matched:

```
redirect context 23 ip host 198.162.100.25 any fragment
```

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

```
before redirect context 23 ip host 198.162.100.25 any fragment
```

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

```
after redirect context 23 ip host 198.162.100.25 any fragment
```

The following deletes the first rule defined above:

```
no redirect context 23 ip host 198.162.100.25 any fragment
```

redirect context (by TCP/UDP packets)

Redirects subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect context *context_id* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port*] }**

after redirect context *context_id* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port*] }**

before redirect context *context_id* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port*] }**

no redirect context *context_id* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port*] }**

after

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

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

before

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

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

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

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

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

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

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

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

dest_host_address

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

eq *source_port*

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

gt *source_port*

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

lt *source_port*

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

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be an integer from 0 through 65535.

dest_address

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

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

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

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be an integer from 0 through 65535.

gt *dest_port*

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

lt *dest_port*

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

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. *dest_port* must be an integer from 0 through 65535.

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of 23, and UDP packets coming from any host are matched:

```
redirect context 23 udp any
```

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

```
before redirect context 23 udp any
```

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

```
after redirect context 23 udp any
```

The following deletes the rule defined above:

```
no redirect context 23 udp any
```

redirect css delivery-sequence

This is a restricted command. In 9.0 and later releases, this command is obsoleted.

redirect css service (any)

Redirects subscriber sessions based on any packet received (Content Service Steering). This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect css service service_name [ log ] any

after redirect css service service_name [ log ] any

before redirect css service service_name [ log ] any

no redirect css service service_name [ log ] any
```

after

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

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

before

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

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

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging all** command to display the names of all configured charging services. *service_name* must be an alphanumeric string from 1 through 15 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any

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

Usage

Define a catch all rule definitions to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

Important: Any rule definition which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

Important: A maximum of 16 rule definitions can be configured per ACL.

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

Example

The following command defines a rule definition that redirects packets to the charging service with the name *chgsvc1* and any source IP:

```
redirect css service chgsvc1 any
```

The following sets the insertion point before the rule definition above:

```
before redirect service chgsvc1 any
```

The following command sets the insertion point after the first rule definitions above:

```
after redirect service chgsvc1 any
```

The following deletes the first rule definition above:

```
no redirect service chgsvc1 any
```

redirect css service (by host IP address)

Redirecst subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *service_name* **[log] host** *source_host_address*

after redirect css service *service_name* **[log] host** *source_host_address*

before redirect css service *service_name* **[log] host** *source_host_address*

no redirect css service *service_name* **[log] host** *source_host_address*

after

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

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

before

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

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

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
service_name must be an alphanumeric string from 1 through 15 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

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

Usage

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *chgsvc1* and a host IP address of *192.168.200.11*:

```
redirect css service chgsvc1 host 192.168.200.11
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 host 192.168.200.11
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 host 192.168.200.11
```

redirect css service (by ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect css service service_name [ log ] icmp { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ icmp_type [ icmp_code ]

before redirect css service service_name [ log ] icmp { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ icmp_type [ icmp_code ]

after redirect css service service_name [ log ] icmp { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ icmp_type [ icmp_code ]

no redirect css service service_name [ log ] icmp { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ icmp_type [ icmp_code ]
```

after

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

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

before

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

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

no

Removes the rule definition which exactly matches the options specified.

`css service` *`service_name`*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **`show active-charging service all`** command to display the names of all configured charging services.
`service_name` must be an alphanumeric string from 1 through 15 characters.

`log`

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

`source_address`

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

`source_wildcard`

This option is used in conjunction with the *`source_address`* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *`source_address`* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *`source_address`* parameter must be ignored.

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

`any`

Specifies that the rule definition applies to all packets.

`host`

Specifies that the rule definition applies to a specific host as determined by its IP address.

`source_host_address`

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

`dest_host_address`

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

`dest_address`

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

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

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

icmp_type

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

icmp_code

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

Usage

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.
The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and ICMP packets coming from the host with the IP address *198.162.100.25*:

```
redirect css service chgsvc1 icmp host 192.168.200.11
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 icmp host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 icmp host 192.168.200.11
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 icmp host 192.168.200.11
```

redirect css service (by IP packets)

Redirects subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect css service service_name [ log ] ip { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ fragment ]

after redirect css service service_name [ log ] ip { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ fragment ]

before redirect css service service_name [ log ] ip { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ fragment ]

no redirect css service service_name [ log ] ip { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ fragment ]
```

after

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

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

before

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

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

no

Removes the rule definition that exactly matches the options specified.

`css service` *`service_name`*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **`show active-charging service all`** command to display the names of all configured charging services.
`service_name` must be an alphanumeric string from 1 through 15 characters.

`log`

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

`source_address`

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

`source_wildcard`

This option is used in conjunction with the *`source_address`* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *`source_address`* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *`source_address`* parameter must be ignored.

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

`any`

Specifies that the rule definition applies to all packets.

`host`

Specifies that the rule definition applies to a specific host as determined by its IP address.

`source_host_address`

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

`dest_host_address`

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

`dest_address`

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

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

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

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

Usage

Block IP packets when the source and destination are of interest.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and IP packets coming from the host with the IP address *198.162.100.25*, and fragmented packets for any destination are matched:

```
redirect css service chgsvc1 ip host 192.168.100.25 any fragment
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 ip host 192.168.100.25 any fragment
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 ip host 192.168.100.25 any fragment
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 ip host 192.168.100.25 any fragment
```

redirect css service (by source IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source to the mobile node or the network (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *service_name* **[log]** *source_address source_wildcard*

after redirect css service *service_name* **[log]** *source_address source_wildcard*

before redirect css service *service_name* **[log]** *source_address source_wildcard*

no redirect css service *service_name* **[log]** *source_address source_wildcard*

after

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

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

before

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

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

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
service_name must be an alphanumeric string from 1 through 15 characters.

log

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

source_address

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

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

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

Usage

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

Important: A maximum of 16 rule definitions can be configured per ACL.

Example

The following command defines a rule definition to redirect packets to a charging service named *chgsvc1*:

```
redirect css service chgsvc1 10.2.3.0 0.0.0.31
```

redirect css service (by TCP/UDP packets)

Redirects subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect css service service_name [ log ] { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt
source_port | neq source_port | range start_source_port end_source_port ] } { {
dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port
| lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }

after redirect css service service_name [ log ] { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt
source_port | neq source_port | range start_source_port end_source_port ] } { {
dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port
| lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }

before redirect css service service_name [ log ] { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt
source_port | neq source_port | range start_source_port end_source_port ] } { {
dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port
| lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }

no redirect css service service_name [ log ] { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt
source_port | neq source_port | range start_source_port end_source_port ] } { {
dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port
| lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
```

after

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

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

before

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

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

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
service_name must be an alphanumeric string from 1 through 15 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

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

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

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

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

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

dest_host_address

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

eq *source_port*

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

gt *source_port*

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

lt *source_port*

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

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

range *start_source_port end_source_port*

Specifies that all source TCP ports within a specific range are to be filtered.
start_source_port is the initial port in the range and *end_source_port* is the final port in the range.
Both *start_source_port* and *end_source_port* can be configured to an integer value from 0 to 65535.

dest_address

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

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

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

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

range *start_dest_port end_dest_port*

Specifies that all destination TCP ports within a specific range are to be filtered.
start_dest_port is the initial port in the range and *end_dest_port* is the final port in the range.
Both *start_dest_port* and *end_dest_port* can be configured to an integer value from 0 to 65535.

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and UDP packets coming from any host are matched:

```
redirect css service chgsvc1 udp any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 udp any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 udp any
```

The following command deletes the rule definition above:

```
no redirect css service chgsvc1 udp any
```

redirect css service (for downlink, any)

Redirects subscriber sessions based on any packet received in the downlink (from the Mobile Node) direction (Content Service Steering). This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *service_name* **[log] downlink any**

after redirect css service *service_name* **[log] downlink any**

before redirect css service *service_name* **[log] downlink any**

no redirect css service *service_name* **[log] downlink any**

after

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

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

before

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

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

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
service_name must be an alphanumeric string from 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any

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

Usage

Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

Important: Any rule definition which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

Important: A maximum of 16 rule definitions can be configured per ACL.

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

Example

The following command defines a rule definition that redirects packets to the charging service with the name *chgsvc1* and any source IP:

```
redirect css service chgsvc1 downlink any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 downlink any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 downlink any
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 downlink any
```

redirect css service (for downlink, by host IP address)

Redirects subscriber sessions based on the targeted host IP address in the downlink (from the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *service_name* **[log] downlink host** *source_host_address*

before redirect css service *service_name* **[log] downlink host** *source_host_address*

after redirect css service *service_name* **[log] downlink host** *source_host_address*

no redirect css service *service_name* **[log] downlink host** *source_host_address*

after

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

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

before

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

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

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
service_name must be an alphanumeric string from 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

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

Usage

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *chgsvc1and* a host IP address of *192.168.200.11*:

```
redirect css service chgsvc1 downlink host 192.168.200.11
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 downlink host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 downlink host 192.168.200.11
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 downlink host 192.168.200.11
```

redirect css service (for downlink, by ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets in the downlink (from the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *service_name* **[log] downlink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**

after redirect css service *service_name* **[log] downlink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**

before redirect css service *service_name* **[log] downlink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**

no redirect css service *service_name* **[log] downlink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**

after

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

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

before

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

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

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
service_name must be an alphanumeric string from 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

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

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

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

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

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

dest_host_address

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

dest_address

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

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

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

icmp_type

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

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.

Usage

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.
The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and ICMP packets coming in the downlink (from the Mobile Node) direction from the host with the IP address 192.168.100.25:

```
redirect css service chgsvc1 downlink icmp host 192.168.100.25
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 downlink icmp host 192.168.100.25
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 downlink icmp host 192.168.100.25
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 downlink icmp host 192.168.100.25
```

redirect css service (for downlink, by IP packets)

Redirects subscriber sessions based on the internet protocol packets in the downlink (from the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *service_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

after redirect css service *service_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

before redirect css service *service_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

no redirect css service *service_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
service_name must be an alphanumeric string from 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

Usage

Block IP packets when the source and destination are of interest.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and downlink IP packets coming from the host with the IP address *198.162.100.25*, and fragmented packets for any destination are matched:

```
redirect css service chgsvc1 downlink ip host 198.162.100.25 any fragment
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 downlink ip host 198.162.100.25 any
fragment
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 downlink ip host 198.162.100.25 any
fragment
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 downlink ip host 198.162.100.25 any
fragment
```

redirect css service (for downlink, by source IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source in the downlink (from the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *service_name* **[log] downlink** *source_address source_wildcard*

after redirect css service *service_name* **[log] downlink** *source_address source_wildcard*

before redirect css service *service_name* **[log] downlink** *source_address source_wildcard*

no redirect css service *service_name* **[log] downlink** *source_address source_wildcard*

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
service_name must be an alphanumeric string from 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

Usage

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Important: A maximum of 16 rule definitions can be configured per ACL.

Example

The following command defines a rule definition to redirect packets to a charging service named *chgsvc1*:

```
redirect css service chgsvc1 downlink 10.2.3.0 0.0.0.31
```

redirect css service (for downlink, by TCP/UDP packets)

Redirects subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the downlink (from the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *service_name* **[log] downlink { tcp | udp } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

after redirect css service *service_name* **[log] downlink { tcp | udp } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

before redirect css service *service_name* **[log] downlink { tcp | udp } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

no redirect css service *service_name* **[log] downlink { tcp | udp } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
service_name must be an alphanumeric string from 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to an integer value from 0 to 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

range *start_source_port end_source_port*

Specifies that all source TCP ports within a specific range are to be filtered.
start_source_port is the initial port in the range and *end_source_port* is the final port in the range.
Both *start_source_port* and *end_source_port* can be configured to an integer value from 0 to 65535.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

range *start_dest_port end_dest_port*

Specifies that all destination TCP ports within a specific range are to be filtered.
start_dest_port is the initial port in the range and *end_dest_port* is the final port in the range.
Both *start_dest_port* and *end_dest_port* can be configured to an integer value from 0 to 65535.

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and UDP packets coming from any host are matched:

```
redirect css service chgsvc1 downlink udp any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 downlink udp any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 downlink udp any
```

The following deletes the rule definition above:

```
no redirect css service chgsvc1 downlink udp any
```

redirect css service (for uplink, any)

Redirects subscriber sessions based on any packet received in the uplink (to the Mobile Node) direction (Content Service Steering). This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *service_name* **[log] uplink any**

after redirect css service *service_name* **[log] uplink any**

before redirect css service *service_name* **[log] uplink any**

no redirect css service *service_name* **[log] uplink any**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
service_name must be an alphanumeric string from 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage

Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

Important: It is suggested that any rule definition which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

Important: A maximum of 16 rule definitions can be configured per ACL.

Important: Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *chgsvc1* and any source IP:

```
redirect css service chgsvc1 uplink any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 uplink any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 uplink any
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 uplink any
```

redirect css service (for uplink, by host IP address)

Redirects subscriber sessions based on the targeted host IP address in the uplink (to the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *service_name* **[log] uplink host** *source_host_address*

after redirect css service *service_name* **[log] uplink host** *source_host_address*

before redirect css service *service_name* **[log] uplink host** *source_host_address*

no redirect css service *service_name* **[log] uplink host** *source_host_address*

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

after

Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

`css service` *`service_name`*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **`show active-charging service all`** command to display the names of all configured charging services.
`service_name` must be an alphanumeric string from 1 through 15 characters.

`uplink`

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

`log`

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

`host`

Specifies that the rule definition applies to a specific host as determined by its IP address.

`source_host_address`

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

Usage

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *`chgsvc1`* and a host IP address of *`192.168.200.11`*:

```
redirect css service chgsvc1 uplink host 192.168.200.11
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 uplink host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 uplink host 192.168.200.11
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 uplink host 192.168.200.11
```

redirect css service (for uplink, by ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets in the uplink (to the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *service_name* **[log] uplink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**

after redirect css service *service_name* **[log] uplink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**

before redirect css service *service_name* **[log] uplink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**

no redirect css service *service_name* **[log] uplink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
service_name must be an alphanumeric string from 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value between 0 and 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.

Usage

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.
The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and ICMP packets in the uplink (to the Mobile Node) direction from the host with the IP address *198.162.100.25*:

```
redirect css service chgsvc1 uplink icmp host 192.168.100.25
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 uplink icmp host 192.168.100.25
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 uplink icmp host 192.168.100.25
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 uplink icmp host 192.168.100.25
```

redirect css service (for uplink, by IP packets)

Redirects subscriber sessions based on the internet protocol packets in the uplink (to the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *service_name* **[log] uplink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

after redirect css service *service_name* **[log] uplink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

before redirect css service *service_name* **[log] uplink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

no redirect css service *service_name* **[log] uplink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
service_name must be an alphanumeric string from 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

Usage

Block IP packets when the source and destination are of interest.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and uplink IP packets going to the host with the IP address *198.162.100.25*, and fragmented packets for any destination are matched:

```
redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 uplink ip host 198.162.100.25 any
fragment
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 uplink ip host 198.162.100.25 any
fragment
```

The following command deletes the first rule definition above:

```
no redirect css service chgsvc1 uplink ip host 198.162.100.25 any
fragment
```

redirect css service (for uplink, by source IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source in the uplink (to the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *service_name* **[log] uplink** *source_address source_wildcard*

after redirect css service *service_name* **[log] uplink** *source_address source_wildcard*

before redirect css service *service_name* **[log] uplink** *source_address source_wildcard*

no redirect css service *service_name* **[log] uplink** *source_address source_wildcard*

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
service_name must be an alphanumeric string from 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Usage

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Example

The following command defines a rule definition to redirect packets to a charging service named *chgsvc1*:

```
redirect css service chgsvc1 uplink 10.2.3.0 0.0.0.31
```

redirect css service (for uplink, by TCP/UDP packets)

Redirects subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the uplink (to the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *service_name* **[log] uplink { tcp | udp } { { *source_address source_wildcard* | **any** | *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

after redirect css service *service_name* **[log] uplink { tcp | udp } { { *source_address source_wildcard* | **any** | *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

before redirect css service *service_name* **[log] uplink { tcp | udp } { { *source_address source_wildcard* | **any** | *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

no redirect css service *service_name* **[log] uplink { tcp | udp } { { *source_address source_wildcard* | **any** | *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
service_name must be an alphanumeric string from 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to an integer value from 0 to 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

range *start_source_port end_source_port*

Specifies that all source TCP ports within a specific range are to be filtered.
start_source_port is the initial port in the range and *end_source_port* is the final port in the range.
Both *start_source_port* and *end_source_port* can be configured to an integer value from 0 to 65535.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

range *start_dest_port end_dest_port*

Specifies that all destination TCP ports within a specific range are to be filtered.
start_dest_port is the initial port in the range and *end_dest_port* is the final port in the range.
Both *start_dest_port* and *end_dest_port* can be configured to an integer value from 0 to 65535.

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and UDP packets coming from any host are matched:

```
redirect css service chgsvc1 uplink udp any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 uplink udp any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 uplink udp any
```

The following deletes the rule definition above:

```
no redirect css service chgsvc1 uplink udp any
```

redirect nexthop (by IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log]** *source_address source_wildcard*

after redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log]** *source_address source_wildcard*

before redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log]** *source_address source_wildcard*

no redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log]** *source_address source_wildcard*

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The directly connected IP address to which the IP packets are forwarded.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 to 79 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

Usage

Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of redirect rules as it does not require a rule for each source and destination pair.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important: Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23 and the source IP and wildcard of 192.168.22.0 and 0.0.0.31:

```
redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

redirect nexthop (any)

Redirects subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**

after redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**

before redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**

no redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The directly connected IP address to which the IP packets are forwarded.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 to 79 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage

Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

Important: Any rule which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important: Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23 and any source IP:

```
redirect nexthop 192.168.10.4 context 23 any
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 any
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 any
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 any
```

redirect nexthop (by host IP address)

Redirects subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
host source_ipv4_address

after redirect nexthop nexthop_addr { context context_id | interface interface_name } [
log ] host source_ipv4_address

before redirect nexthop nexthop_addr { context context_id | interface interface_name } [
log ] host source_ipv4_address

no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log
] host source_ipv4_address
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The directly connected IP address to which the IP packets are forwarded.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 to 79 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_ipv4_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

Usage

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important: Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23 and a host IP address of 192.168.200.11:

```
redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

redirect nexthop (by source ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
icmp { source_address source_wildcard | any | host source_host_address } { dest_address
dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

after redirect nexthop nexthop_addr { context context_id | interface interface_name } [
log ] icmp { source_address source_wildcard | any | host source_host_address } {
dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

before redirect nexthop nexthop_addr { context context_id | interface interface_name } [
log ] icmp { source_address source_wildcard | any | host source_host_address } {
dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log
] icmp { source_address source_wildcard | any | host source_host_address } { dest_address
dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The directly connected IP address to which the IP packets are forwarded.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 through 79 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value between 0 and 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.

Usage

Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk. The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important: Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23, and ICMP packets coming from the host with the IP address 198.162.100.25:

```
redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```

redirect nexthop (by IP packets)

Redirects subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
ip { source_address source_wildcard | any | host source_host_address } { dest_address
dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]

after redirect nexthop nexthop_addr { context context_id | interface interface_name } [
log ] ip { source_address source_wildcard | any | host source_host_address } {
dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]

before redirect nexthop nexthop_addr { context context_id | interface interface_name } [
log ] ip { source_address source_wildcard | any | host source_host_address } {
dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]

no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log
] ip { source_address source_wildcard | any | host source_host_address } { dest_address
dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The directly connected IP address to which the IP packets are forwarded.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 through 79 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

protocol *num*

Indicates that the packet filtering is to be applied to a specific protocol number.
num can be an integer ranging from 0 to 255.

Usage

Block IP packets when the source and destination are of interest.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important: Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23, and IP packets coming from the host with the IP address 198.162.100.25, and fragmented packets for any destination are matched:

```
redirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25 any
fragment
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25
any fragment
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25 any
fragment
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25 any
fragment
```

redirect nexthop (by TCP/UDP packets)

Redirects subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] {
tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq
source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address
dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt
dest_port | neq dest_port ] }

after redirect nexthop nexthop_addr { context context_id | interface interface_name } [
log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address }
[ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address
dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt
dest_port | neq dest_port ] }

before redirect nexthop nexthop_addr { context context_id | interface interface_name } [
log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address }
[ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address
dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt
dest_port | neq dest_port ] }

no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log
] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [
eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address
dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt
dest_port | neq dest_port ] }
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The directly connected IP address to which the IP packets are forwarded.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 through 79 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.
source_port must be an integer from 0 through 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be an integer from 0 through 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be an integer from 0 through 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be an integer from 0 through 65535.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be an integer from 0 through 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
dest_port must be an integer from 0 through 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.
dest_port must be an integer from 0 through 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.
dest_port must be an integer from 0 through 65535.

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important: Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23, and UDP packets coming from any host are matched:

```
redirect nexthop 192.168.10.4 context 23 udp any
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 udp any
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 udp any
```

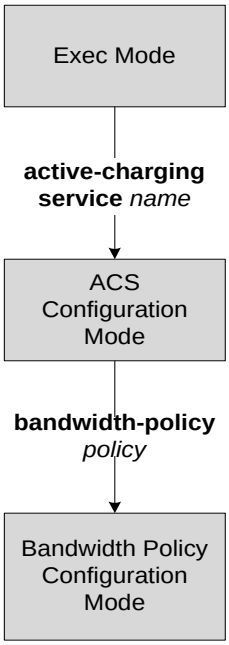
The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 udp any
```

- redirect nexthop (by TCP/UDP packets)

Chapter 6
ACS Bandwidth Policy Configuration Mode Commands

The ACS Bandwidth Policy Configuration Mode is used to create and manage Active Charging Service (ACS) Bandwidth Policies.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

flow limit-for-bandwidth

This command allows you to configure the flow limit-for-bandwidth parameter for the current bandwidth policy.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

flow limit-for-bandwidth id *bandwidth_id* **group-id** *group_id*

no flow limit-for-bandwidth id *bandwidth_id*

no

If previously configured, removes the specified flow limit-for-bandwidth configuration in the current bandwidth policy.

id *bandwidth_id*

Specifies ID for the current bandwidth policy.
bandwidth_id must be an integer from 1 through 65535.

group-id *group_id*

Specifies group ID for the current bandwidth policy.
group_id must be an integer from 1 through 65535.

Usage

Use this command to configure the flow limit-for-bandwidth configuration for a bandwidth policy.

Example

The following command configures the Flow Limit-for-Bandwidth configuration with bandwidth policy ID *test123* and group ID *123*:

```
flow limit-for-bandwidth id test123 group-id 123
```

group-id

This command allows you to configure the group ID for the current bandwidth policy.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

group-id *group_id* **direction { downlink | uplink } peak-data-rate** *peak_data_rate* **peak-burst-size** *peak_burst_size* **violate-action { discard | lower-ip-precedence } [committed-data-rate** *committed_data_rate* **committed-burst-size** *committed_burst_size* **[exceed-action { discard | lower-ip-precedence }]]**

{ default | no } group-id *group_id* **direction { downlink | uplink }**

default

Configures this command with default settings for the specified group ID.

no

If previously configured, removes the specified group ID configuration from the current bandwidth policy.

group_id

Specifies the group ID.
group_id must be an integer from 1 through 65535.

direction { downlink | uplink }

Specifies the direction for which bandwidth will be controlled.

peak-data-rate *peak_data_rate*

Specifies the peak data rate, in bits per second.
peak_data_rate must be an integer from 1 through 4294967295.
Default: 0

peak-burst-size *peak_burst_size*

Specifies the peak burst size, in bytes.
peak_burst_size must be an integer from 1 through 4294967295.
Default: 0

violate-action { discard | lower-ip-precedence }

Specifies the action to be taken if Peak Data Rate is surpassed.

- **discard**: Specifies to discard the packet
- **lower-ip-precedence**: Specifies to lower IP precedence of the packet

committed-data-rate *committed_data_rate*

Specifies the committed Data Rate, in bits per second. This can also be used to specify the Guaranteed Bit Rate (GBR) for Network Controlled QoS (NCQoS) without exceed-action.
committed_data_rate must be an integer from 1 through 4294967295.
Default: 0

committed-burst-size *committed_burst_size*

Specifies the committed burst size, in bytes.
committed_burst_size must be an integer from 1 through 4294967295.
Default: 0

exceed-action { discard | lower-ip-precedence }

Specifies the action to be taken if Committed Data Rate is surpassed.

- **discard**: Specifies to discard the packet.
- **lower-ip-precedence**: Specifies to lower IP precedence of the packet.

Usage

Use this command to configure the Group ID for an bandwidth policy.

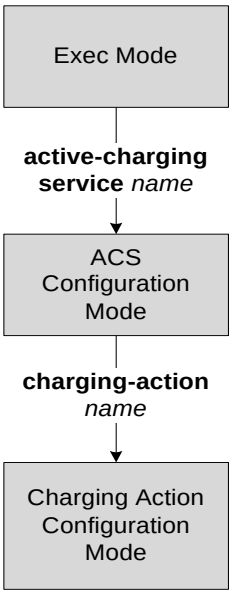
Example

The following command configures the group ID *111* to control bandwidth in the downlink direction specifying peak data rate of *10000* bits per second and peak burst size of *10000* bytes while specifying the action to be taken on violation as discard:

```
group-id 111 direction downlink peak-data-rate 10000 peak-burst-size
10000 violate-action discard
```

Chapter 7
ACS Charging Action Configuration Mode Commands

The ACS Charging Action Configuration Mode is used to configure Active Charging Service (ACS) charging actions.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

allocation-retention-priority

This command allows you to configure the Allocation Retention Priority (ARP).

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
allocation-retention-priority priority [ pci pci_value | pvi pvi_value ]

no allocation-retention-priority
```

no

If previously configured, disables ARP configuration in the current charging action.

priority

priority must be an integer from 1 through 15.

pci *pci_value*

Specifies the Pre-emption Capability Indicator (PCI).
pci_value must be integer 0 or 1.

Important: If not explicitly enabled, then the default value of 1 will hold true.

pvi *pvi_value*

Specifies the Pre-emption Vulnerability Indicator (PVI).
pvi_value must be integer 0 or 1.

Important: If not explicitly enabled, then the default value of 0 will hold true.

Usage

This command configures the ARP, which indicates the priority of allocation and retention of the service data flow. The ARP resolves conflicts in demand for network resources. At the time of resource crunch, this parameter prioritizes allocation of resources during bearer establishment and modification. In a congestion situation, a lower ARP flow may be dropped to free up capacity. Once a service flow is successfully established, this parameter plays no role in quality of service (QoS) experienced by the flow.

Example

The following command sets the ARP to *10*:

```
allocation-retention-priority 10
```

billing-action

This command allows you to configure the billing action for packets that match specific rule definitions (ruledefs).

Product

All

Privilege

Security Administrator, Administrator

Syntax

In 12.1 and earlier releases:

```
billing-action { edr edr_format_name [ wait-until-flow-ends ] | egcdr | exclude-from-udrs
| radius | rf } +

no billing-action [ edr | egcdr | exclude-from-udrs | radius | rf ] +
```

In 12.2 and later releases:

```
billing-action { create-edrs { charging-edr charging_edr_format_name | reporting-edr
reporting_edr_format_name } + [ wait-until-flow-ends ] | egcdr | exclude-from-udrs |
radius | rf } +

no billing-action [ create-edrs | egcdr | exclude-from-udrs | radius | rf ] +
```

no

If previously configured, disables the specified configuration in the current charging action.

edr *edr_format_name* **[wait-until-flow-ends]**

Important: This option is available only in 12.1 and earlier releases. In 12.2 and later releases, it is deprecated and is replaced by the **create-edrs charging-edr** option.

Enables EDR billing for packets matching this charging action.
edr_format_name must be the name of an existing EDR format, and must be an alphanumeric string of 1 through 63 characters.

Important: If the EDR format name specified here is not configured in the EDR Format Configuration Mode, or has been deleted, the system accepts it without applying any EDR format for the billing action in this ACS service.

If this option is configured, the system generates an EDR immediately when a packet is received and it matches a ruledef that is associated with this charging action. Other events configured for flow end-condition, flow action, termination, and/or session control also create the triggers for EDR generation.
wait-until-flow-ends: By default, the EDR is generated immediately after a ruledef hit results in this charging action. When this keyword is specified, no EDR is generated on a ruledef hit. When the flow ends, an attempt is made to generate an EDR with the format specified.

create-edrs { charging-edr *charging_edr_format_name* **| reporting-edr** *reporting_edr_format_name* **} + [wait-until-flow-ends]**

Important: This option is available only in 12.2 and later releases.

Enables EDR billing for packets matching this charging action.

- **charging-edr** *charging_edr_format_name*: Specifies to generate charging EDR.

  charging_edr_format_name must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

- **reporting-edr** *reporting_edr_format_name*: Specifies to generate reporting EDR.

  reporting_edr_format_name must be the name of a reporting EDR format, and must be an alphanumeric string of 1 through 63 characters.

If the above options are configured, the system generates an EDR immediately when a packet is received and it matches a ruledef that is associated with this charging action. Other events configured for flow end-condition, flow action, termination, and/or session control also creates the triggers for EDR generation.

- **wait-until-flow-ends**: By default, the EDR is generated immediately after a ruledef hit results in this charging action. When this keyword is specified, no EDR is generated on a ruledef hit. When the flow ends, an attempt is made to generate an EDR with the format specified.

egcdr

Enables eG-CDR billing for packets matching this charging action.
If this option is configured, the system generates an eG-CDR when the subscriber session ends or an interim trigger condition occurs. The interim triggers are configurable in the ACS Rulebase Configuration Mode. In addition, whenever there is an SGSN-to-SGSN handoff the system treats that as a trigger.
To generate an eG-CDR the **accounting-mode** command in the APN Configuration Mode must be configured with the "none" option.
The format of enhanced G-CDRs is controlled by the **inspector** CLI command in the Context Configuration Mode.

exclude-from-udrs

By default, statistics are accumulated on a per content ID basis for possible inclusion in UDRs. The **exclude-from-udrs** keyword causes the system to not include the packet's statistics in UDRs.
When this option is disabled, (the default setting) UDRs will be generated based on the UDR format specified in the rulebase.
Default: Disabled.

radius

Enables billing action as RADIUS Charging Data Records (CDRs) for packets matching this charging action, and the data packet statistics will be included in the postpaid RADIUS accounting.
Default: Disabled.

rf

Enables Rf accounting.
Rf accounting is applicable only for dynamic and predefined rules that are marked for it. Dynamic rules have a field offline-enabled to indicate this. To mark a predefined rule as offline-enabled, use this keyword and the **billing-records** CLI in the ACS Rulebase Configuration Mode.

Usage

Use this command to enable an EDR, eG-CDR and/or RADIUS CDR type of billing for content matching this charging action.

Example

in 12.1 and earlier releases, the following command enables the EDR billing type with EDR format *charge1_format*:

```
billing-action edr charge1_format
```

In 12.2 and later releases, the following command is applied to both charging and reporting EDRs since the trigger for both the EDRs is the same:

```
billing-action create-edrs charging-edr charging_edrformat1 reporting-edr
reporting_edrformat1 wait-until-flow-ends
```

cca charging credit

This command allows you to enable/disable Credit Control Application (CCA) and configure the RADIUS/Diameter prepaid charging behavior.

Product

All

Privilege

Security Administrator, Administrator

Syntax

cca charging credit [rating-group *coupon_id* **] [preemptively-request]**

{ default | no } cca charging

no

If previously configured, disables RADIUS/Diameter Prepaid Credit Control Charging in the current charging action.

default

Disables RADIUS/Diameter Prepaid Credit Control Charging.

credit

Specifies RADIUS/Diameter Prepaid Credit Control Charging Credit behavior.

preemptively-request

Specifies RADIUS/Diameter prepaid credit preemptively requested charging credit behavior. If this option is used, a quota is requested for the specific type of content during session initialization.

rating-group *coupon_id*

Specifies the coupon ID used in prepaid charging as rating-group which maps to the coupon ID for prepaid customer.
coupon_id must be an integer from 0 through 65535.
This option also assigns different content-types for the same charging action depending upon whether or not prepaid is enabled.

Important: This rating-group overrides the content ID, if present in the same charging-action for the prepaid customer in Diameter Credit Control Application (DCCA). But only the content IDs will be used in eG-CDRs irrespective of the presence of rating-group in that charging action.

Usage

Use this command to configure RADIUS/Diameter Prepaid Credit Control Charging behavior.
This command selects reservation based credit control. A CCR-Initial is used to reserve quota upon the first traffic, then a series of CCR-updates are issued as the traffic proceeds and quota dwindles. A CCR-Terminate is issued at the end of the session or at the end of the quota-hold-time.

Example

The following is an example of this command:

```
cca charging credit
```

charge-units

This command allows you to configure the charge units for RADIUS/DCCA charging calculation.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

charge-units *units*

{ default | no } charge-units

default

Configures this command with its default setting.
Default: 0; disables the counter, same as **no charge-units**

no

If previously configured, disables the charge-units configuration in the current charging action.

units

Specifies the service-specific fixed unit counter per content ID for RADIUS/DCCA charging.
units is the value set for charging unit, and must be an integer from 1 through 65535.

Usage

This command configures the unit amount counters for charging calculation on per content ID basis for different protocols and packets regardless of packet direction (uplink or downlink).

Important: For more information on content ID, refer to the **if-protocol** command in the *ACS Ruledef Configuration Mode Commands* chapter.

Example

The following command sets the charging unit to *1024*:

```
charge-units 1024
```

charge-volume

This command allows you to configure how the volume amount counter for eG-CDRs, UDRs, and DCCA charging are calculated.

Product

All

Privilege

Security Administrator, Administrator

Syntax

charge-volume { { dns | ftp-control | ftp-data | http | icmp | imap | ip | mms | pop3 | pptp | rtcp | rtp | rtsp | sdp | secure-http | sip | smtp | tcp | tftp | udp | wsp | wtp } { bytes | packet-length | packets } [downlink | uplink] | constant *fixed_value* **}**

{ default | no } charge-volume

---

default

Configures this command with its default setting.
Default: **charge-volume ip bytes**

---

no

If previously configured, deletes the charge-volume configuration in the current charging action.

{ dns | ftp-control | ftp-data | http | icmp | imap | ip | mms | pop3 | pptp | rtcp | rtp | rtsp | sdp | secure-http | sip | smtp | tcp | tftp | udp | wsp | wtp }

Specifies the charge volume method for the specific rule definition.

- **dns**: Charge volume for DNS
- **ftp-control**: Charge volume for FTP-Control
- **ftp-data**: Charge volume for FTP-Data
- **http**: Charge volume for HTTP
- **icmp**: Charge volume for ICMP
- **imap**: Charge volume for Internet Message Access Protocol (IMAP)
- **ip**: Charge volume for IP
- **mms**: Charge volume for MMS
- **pop3**: Charge volume for POP3
- **pptp**: Charge volume for PPTP
- **rtcp**: Charge volume for RTCP
- **rtp**: Charge volume for RTP
- **rtsp**: Charge volume for RTSP
- **sdp**: Charge volume for SDP
- **secure-http**: Charge volume for secure-https

- **sip**: Charge volume for SIP
- **smtp**: Charge volume for SMTP
- **tcp**: Charge volume for TCP
- **tftp**: Charge volume for TFTP
- **udp**: Charge volume for UDP
- **wsp**: Charge volume for WSP
- **wtp**: Charge volume for WTP

bytes

Sets charge volume for bytes.

packet-length

Sets charge volume for packet length.

packets

Sets charge volume for packets.

constant *fixed_value*

This sets the fixed increment value for charging.
fixed_value is the value set for charging, and must be an integer from 0 through 65535.
If **constant** *3* is configured for every invocation of this Charging Action, the system adds 3 to the downlink/uplink volume counter, depending on the direction of packet.

Usage

This command provides the method for charging volume calculation for different protocols and packets.
For information on supported protocols see the *ACS Ruledef Configuration Mode Commands* chapter.
If **charge-volume rtp packets** is configured, system computes volume amounts for different options for RTP as follows:

Volume	Description
Volume amount	Total (downlink and uplink) RTP packets
Volume amount uplink	Uplink RTP packets
Volume amount downlink	Downlink RTP packets
Volume amount uplink packets	Uplink RTP packets
Volume amount downlink packets	Downlink RTP packets
Volume amount uplink bytes	Uplink RTP bytes
Volume amount downlink bytes	Downlink RTP bytes

Important: Whenever service counts volume, it counts all packets that the relevant analyzers accepted.

Important: If a TCP packet is routed to the HTTP analyzer but there is no HTTP payload, then the TCP statistics will be updated but the HTTP statistics will not be updated (except for the "packets ignored by the HTTP analyzer" statistic).

Example

Following command sets the charging volume of downlink packets for RTP:

```
charge-volume rtp packets downlink
```

content-filtering processing server-group

This command allows you to enable/disable Category-based Content Filtering.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

```
content-filtering processing server-group

{ default | no } content-filtering processing
```

default

Configures this command with its default setting.
Default: Content filtering configured for the rulebase is attempted

no

Specifies to bypass content filtering.
This configuration should only be specified for charging actions that are performed when known safe sites are being accessed.

Usage

Use this command to enable or disable Category-based Content Filtering in the charging action.
This command works as second-level filter to process the HTTP/WAP GET request with Internet Content Adaptation Protocol (ICAP) after ruledef matching. The first-level filtering is in the rulebase configuration.
This CLI command is only effective when the **content-filtering mode server-group** command is configured in the rulebase.

Example

The following command enables content filtering in the current charging action:

```
content-filtering processing server-group
```

content-id

This command allows you to specify the content ID to use in the generated billing records, as well as the AVP used by the Credit Control Application, such as the "Rating-Group" AVP for use by the Diameter Credit Control Application (DCCA).

Product

All

Privilege

Security Administrator, Administrator

Syntax

content-id *content_id*

no content-id

no

Removes the content ID configuration from the charging action.

content_id

Specifies the content ID for credit control service.
In 12.1 and earlier releases *content_id* must be an integer from 1 through 65535.
In 12.2 and later releases, *content_id* must be an integer from 1 through 2147483647.

Usage

This command specifies an optional content ID to use in the generated billing records. This identifier assists the carrier's billing post processing and also used by credit-control system to use independent quotas for different value of **content-id**.
If the specified ruledef uses the **if-protocol** command to select a value for content ID, then the *content_id* specified through this command is not used for billing record generation.

Important: For more information on **content-id**, refer to the **if-protocol** command in the *ACS Ruledef Configuration Mode Commands* chapter.

Example

The following command sets the content ID in the current charging action to *23*:

```
content-id 23
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

fair-usage

This command allows you to enable/disable the fair usage credit system for the Mobile Video Gateway's dynamic inline transrating feature CAC (Call Admission Control) policy. The fair usage credit system enforces a maximum number of video clips that can be dynamically transrated at the same time by allocating an equal number of transrating credits to all the ACS managers in the system.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] fair-usage [ cpu-only | cpu-param { threshold-percent } | deact-margin |
memory-only | threshold-percent ]
```

default

Resets the fair usage settings to their default values.

no

Disables the fair usage credit system for dynamic inline transrating if previously configured.

fair-usage

Enables the fair usage credit system for the CAC policy and applies it to the system CPUs and memory.

cpu-only

Enables the fair usage credit system for the CAC policy and applies it to the system CPUs only.

cpu-param { threshold-percent }

Specifies the percent of system CPU resources that the dynamic inline transrating feature is allowed to use, which can be between 1 and 100 percent. CPU usage above this threshold percent starts the monitor action, which disallows additional video requests to be transrated. By default, this value is set to 10 percent when fair usage is enabled.

deact-margin

Specifies the deactivate margin in percent, below which the monitor action is disabled.

memory-only

Enables the fair usage credit system for the CAC policy and applies it to system memory only.

threshold-percent

Specifies the percent of system resources that the dynamic inline transrating feature is allowed to use, which can be between 1 and 100 percent. This threshold percent is used to start the monitor action, which disallows additional video requests to be transrated. By default, this value is set to 10 percent when fair usage is enabled.

Usage

Use this command to enable the fair usage credit system for the dynamic inline transrating feature CAC policy on the Mobile Video Gateway.

Example

The following command enables the fair usage credit system for the dynamic inline transrating feature CAC policy and applies it to the system CPUs only:

```
fair-usage cpu-only
```

flow action

This command allows you to specify the action to take on packets that matched rule definitions.

Product

All

Privilege

Security Administrator, Administrator

Syntax

In 12.1 and earlier releases:

flow action { conditional user-agent end-token *end_token_name* **| discard [downlink | uplink] | random-drop interval** *interval_start* **to** *interval_end* **pkts-to-drop** *packet_min* **to** *packet_max* **| redirect-url** *redirect_url* **[clear-quota-retry-timer] | readdress [server** *ipv4_address* **] [port** *port_number* **] | terminate-flow | terminate-session }**

no flow action

In 12.2 and later releases:

flow action { conditional user-agent end-token *end_token_name* **| discard [downlink | uplink] | random-drop interval** *interval_start* **to** *interval_end* **pkts-to-drop** *packet_min* **to** *packet_max* **| readdress [server** *ipv4_address* **] [port** *port_number* **] | redirect-url** *redirect_url* **[[encryption { blowfish128 | blowfish64 } [encrypted] key** *key* **] clear-quota-retry-timer] | terminate-flow | terminate-session }**

no flow action

---

no

If previously configured, deletes the flow action configuration in the current charging action.

---

conditional user-agent end-token *end_token_name*

Specifies to conditionally redirect the HTTP packets matched to a configured user-agent to a specified URL. The user agent is configured using the **redirect user-agent** command in the ACS Configuration Mode. *end_token_name* must be an alphanumeric string of 1 through 32 characters, and is configured with this command to end the redirection condition.

---

discard [downlink | uplink]

Specifies to discard the specified packets.

- **downlink**: Downlink packets
- **uplink**: Uplink packets

If **downlink** or **uplink** keyword is not specified, both downlink and uplink packets will be discarded.

---

random-drop interval *interval_start* **to** *interval_end* **pkts-to-drop** *packet_min* **to** *packet_max*

Specifies to drop a group of consecutive packets (**pkts-to-drop**) to be dropped in the specified time interval (**random-drop interval**). This will cause degradation in user experience. P2P VoIP would need

more than one packet to be dropped, since that type of protocol is geared to handle occasional single packet drops.

- **random-drop interval** *interval_start* **to** *interval_end*: Specifies the random drop interval, in seconds, at which the voice packets will be dropped.

  interval_start and *interval_end* must be integers from 1 through 999.

- **pkts-to-drop** *packet_min* **to** *packet_max*: Specifies the number of voice packets to be dropped at a time in a flow when the packets have to be dropped.

  packet_min and *packet_max* must be integers from 1 through 100.

---

readdress { server *ipv4_address* **[port** *port_number* **] | port** *port_number***}**

Specifies to readdress (change the destination address) uplink packets, and optionally the destination TCP/UDP port number. Or, you can keep the original destination address and just change the destination TCP/UDP port number.

- *ipv4_address* specifies the re-address server's IPv4 address.
- *port_number* must be the re-address server's port number, and must be an integer from 1 through 65535.

---

redirect-url *redirect_url* **[[encryption { blowfish128 | blowfish64 } [encrypted] key** *key* **] clear-quota-retry-timer]**

Specifies to return a redirect response to the subscriber, and terminate the TCP connections (to the subscriber and server). The subscriber's Web browser should automatically send the original HTTP packet to the specified URL. Redirection is only possible for certain types of HTTP packets (for example, GET requests), which typically are only sent in the uplink direction. If the flow is not HTTP, the **redirect-url** option is ignored, that is the packet is forwarded normally, except for SIP. For SIP, a Contact header with the redirect information is inserted.

- *redirect_url* specifies the redirect URL. *redirect_url* must be an alphanumeric string of 1 through 511 characters. It may include one or more dynamic fields (up to 16 may be specified). For example, *http://search.com/subtarg=#HTTP.URL#*.

  Dynamic fields must be enclosed in "#" (hash).

  Up to 16 dynamic fields out of the following 23 are allowed:

  - #BEARER.CALLED-STATION-ID#
  - #BEARER.CALLING-STATION-ID#
  - #BEARER.NAS-IP-ADDRESS#
  - #BEARER.USER-NAME#
  - #BEARER.ACCT-SESSION-ID#
  - #BEARER.CORRELATION-ID#
  - #BEARER.RULEBASE#
  - #BEARER.SERVED-BSA-ADDR#
  - #BEARER.SERVICE-NAME#
  - #BEARER.SUBSCRIBER-ID#
  - #BEARER.MSISDN#
  - #HTTP.URL#
  - #HTTP.URI#

- #HTTP.HOST#
- #RTSP.URI#
- #WSP.URL#
- #CONTENT-ID-LABEL#
- #CONTENT-ID-LABEL-CAUSING-REDIRECTION#
- #BEARER.HWID#
- #BEARER.IMSI#
- #BEARER.IMEI#
- #BEARER.ESN#
- #BEARER.MEID#

Concatenated fields separated by ';' can also be inserted. For example, #BEARER.IMSI;BEARER.IMEI#

- **encryption**: Specifies to enable encryption for dynamic fields of redirect URL.
  - **blowfish128**: Specifies to use Blowfish encryption with 28 bit key for encrypting the dynamic fields.
  - **blowfish64**: Specifies to use Blowfish encryption with 64 bit key for encrypting the dynamic fields.
- **encrypted**: Specifies to encrypt the key.
- **key** *key*: Specifies key to use for encryption of dynamic fields.

  key must be an alphanumeric string of 1 through 523 characters.
- **clear-quota-retry-timer**: Specifies to reset Credit Control Application (CCA) Quota Retry Timer upon redirection.

Note that encryption is supported only for the following fields:

- #BEARER.MSISDN#
- #BEARER.CALLING-STATION-ID#
- #BEARER.MSISDN#
- #BEARER.IMEI#
- #BEARER.MEID#
- #BEARER.IMSI#
- #BEARER.USERNAME#
- #BEARER.ESN#

Also, concatenated fields having any of the above will be encrypted.
`%3furl=` can be used as a delimiter between URL. As in `http://search.com/subtarg/%3furl=#HTTP.URL#` format.

---

terminate-flow

Specifies to terminate the flow.
Terminates the TCP connection gracefully between the subscriber and external server and sends a TCP FIN to the subscriber and a TCP RST to the server. If the flow does not use TCP, this option simply discard the packets. This option is applicable only for flows that use TCP.

terminate-session

Specifies to terminate the session.
When a rule pointing to a charging action configured with the terminate-session keyword is hit, then the corresponding session will be terminated.

Usage

Use this command to specify the action to take on packets, for example to discard, terminate, or redirect.
When a readdress server is configured for a charging action, the **show configuration** command will display the readdress related configuration only if server address is configured. The **show configuration verbose** command will display the readdress sever if configured, else will display "no flow action".
The redirect-url option can be used to redirect SIP requests as well. The following is a sample configuration:

```
configure
   active-charging service s1
      charging-action ca_sip_redir
         content-id 10
         flow action redirect-url sip:test@sip.org
         exit
      ruledef sip_req
         sip request packet = TRUE
         exit
      rulebase plan1
         action priority 08 ruledef sip_req charging-action ca_sip_redir
         /* other rules, routing rules for sip, etc */
         end
```

This would mean any SIP request that hits the *sip_req* ruledef, would get redirected to the url given in *ca_sip_redir*. This involves creating a redirection packet with the following response line and "Contact" header in the response.
SIP/2.0 302 Moved Temporarily
302 Moved Temporarily
Most of the header fields are copied directly from the request, so that the mandatory SIP headers are present. If content-length header was seen in the original message, it is replaced in the reply with "Content-Length: 0".

Example

The following command sets the flow action to terminate:

```
flow-action terminate-flow
```

The following command resets quota retry timer upon redirection of flow to HTTP URL *http://search.com/?url=#http://msn.com#*:

```
flow action redirect-url http://search.com/%3url=#http://msn.com# clear-
quota-retry-timer
```

flow idle-timeout

This command allows you to configure the maximum duration a flow can remain idle after which the system automatically terminates the flow.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
flow idle-timeout { idle_timeout | flow-mapping flow_timeout }

{ default | no } flow idle-timeout [ flow-mapping ]
```

no

Disables the idle-timeout configuration; sets the idle-timeout to 0 seconds.

default

Configures this command with its default setting.
Default: 300 seconds

idle-timeout *idle_timeout*

Specifies the maximum duration, in seconds, a flow can remain idle.
idle_timeout must be an integer from 0 through 86400.

flow-mapping *flow_timeout*

Specifies the maximum duration of flow-mapping timeout, in seconds.
flow_timeout must be an integer from 0 through 86400.

Usage

Use this command to configure the maximum duration a flow can remain idle after which the system automatically terminates the flow.

Example

The following command configures the idle-timeout setting to *400* seconds:

```
flow idle-timeout 400
```

flow limit-for-bandwidth

For Session Control functionality this command allows you to enable/disable bandwidth limiting and configure the uplink and downlink bandwidth limits for subscriber.

Product

All

Privilege

Security Administrator, Administrator

Syntax

flow limit-for-bandwidth { { direction { downlink | uplink } peak-data-rate *bps* **peak-burst-size** *bytes* **violate-action { discard | lower-ip-precedence } [committed-data-rate** *bps* **committed-burst-size** *bytes* **[exceed-action { discard | lower-ip-precedence }]] } | { id** *id* **} }**

{ default | no } flow limit-for-bandwidth { direction { downlink | uplink } | id }

no

If previously configured, disables bandwidth control traffic policing for the specified direction for the current subscriber.

default

Configures this command with its default setting.

direction { downlink | uplink }

Specifies the direction of flow to apply bandwidth limit:

- **downlink**: Flow of data towards subscriber.
- **uplink**: Flow of data from subscriber.

peak-data-rate *bps*

Specifies the peak data-rate for the subscriber, in bps (bits per second).
bps must be an integer from 1 through 4294967295.
Default: 256000

peak burst-size *bytes*

The peak burst size allowed, in bytes.
bytes must be an integer from 1 through 4294967295.
Default: 3000

Important: It is recommended that this parameter be configured to at least the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.

violate-action { discard | lower-ip-precedence }

Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **discard**: Discard the packet
- **lower-ip-precedence**: Transmit the packet after lowering the IP precedence

Default: **discard**

committed-data-rate *bps*

The committed data rate (guaranteed-data-rate) in bits per second (bps).
bps must be an integer from 1 through 4294967295.
Default: 144000

committed-burst-size *bytes*

The committed burst size allowed, in bytes.
bytes must be an integer from 1 through 4294967295.
Default: 3000

exceed-action { discard | lower-ip-precedence }

The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

- **discard**: Discard the packet
- **lower-ip-precedence**: Transmit the packet after lowering the ip-precedence

If exceed-action is not configured, the packets are forwarded.
Default: **lower-ip-precedence**

id *id*

Important: This keyword is only available in 8.1 and later releases.

Specifies the bandwidth limiting identifier.
id must be an integer from 1 through 65535.
This identifier enables traffic policing based on a separate identifier other than content ID. This identifier will always take priority over content ID. If this identifier is not configured, traffic policing will be based on the content ID.

Usage

Use this command to limit the bandwidth a subscriber uses in the uplink and downlink directions under Session Control.

Important: If the exceed/violate action is set to "lower-ip-precedence", the TOS value for the outer packet becomes "best effort" for packets that exceed/violate the traffic limits regardless of what the **ip user-datagram-tos copy** command is configured to. In addition, the **lower-ip-precedence** option may also override the **ip qos-dscp** command configuration. Therefore, it is recommended that command not be used when specifying this option.

More information on the QoS feature is available in the *QoS Management* appendix of the *System Administration Guide*.

Example

The following command sets an uplink peak data rate of *128000* bps and lowers the IP precedence when the committed-data-rate and the peak-data-rate are exceeded:

```
flow limit-for-bandwidth uplink peak-data-rate 128000 violate-action
lower-ip-precedence
```

The following command sets a downlink peak data rate of *256000* bps and discards the packets when the committed-data-rate and the peak-data-rate are exceeded:

```
flow limit-for-bandwidth downlink peak-data-rate 256000 violate-action
discard
```

flow limit-for-flow-type

This command allows you to specify the maximum number of simultaneous flows (of this type) that a subscriber may have, and the action to take if the limit is reached.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
flow limit-for-flow-type limit over-limit-action { discard | redirect-url | terminate-flow | terminate-session }

no flow limit-for-flow-type
```

no

If previously configured, deletes the flow limit-for-flow-type configuration in the current charging action.

limit

Specifies the maximum number of flows of a type exceeding which the specified over-limit-action triggers. *limit* must be an integer from 1 through 4000000000.

over-limit-action { discard | redirect-url | terminate-flow | terminate-session }

Specifies the action to take on exceeding *limit* for a flow type:

- **discard**: Discards the packets
- **redirect-url**: Redirects the flow
- **terminate-flow**: Terminates the flow to which this packet belongs
- **terminate-session**: Terminates the session to which this packet belongs

Usage

Use this command to specify the number of simultaneous flows (of a type) that a subscriber may have, and the action to take if the limit is reached.
All flows with the same content-id are considered to be the same type. This limit applies to the total of all flows for a subscriber connection (that is, an individual PDP context or individual A10 tunnel).
If the flow is not HTTP, the **redirect-url** option is ignored, that is the packet is forwarded normally. Refer to the **flow action** CLI command.
If the limit specified by the **flow limit-across-applications** command in the Rulebase Configuration Mode is also exceeded, action is taken for that over-limit condition rather than the action configured here.

Example

The following command terminates the flow if total number of flows of a type exceeds *1024*:

```
flow limit-for-flow-type 1024 over-limit-action terminate-flow
```

ip tos

This command allows you to configure the IP Type of Service (ToS) octets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
ip tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 |
af43 | be | ef | lower-bits tos_value } [ uplink | downlink ]

{ default | no } ip tos [ uplink | downlink ]
```

default

Configures this command with its default setting.
Default: IP ToS is not modified.

no

If previously configured, deletes the IP ToS configuration in the current charging action.

af *xx*

Specifies the use of an assured forwarding *xx* per hop behavior (PHB).

be

Specifies the use of best effort forwarding PHB.

ef

Specifies the use of expedited forwarding PHB.

lower-bits *tos_value*

Important: In StarOS 8.1 and later releases, this keyword is "**lower-bits** *tos_value*". In StarOS 8.0, it is *tos_value*.

Specifies the least-significant 6 bits in the TOS byte with the specified numeric value.
tos_value must be an integer from 0 through 63.

downlink

Specifies the ToS only for downlink packets.

uplink

Specifies the ToS only for uplink packets.

Usage

Use this command to specify the IP Type of Service (ToS) octets to use in the charging action. If one of the enumerated values is set, the DSCP bits which are the six most-significant bits in the TOS byte are marked. If the integer value is set, it will be written into the six least-significant bits of the TOS byte.
If **downlink** or **uplink** keywords are not specified, the command applies to both directions.
This command may be used multiple times. For example, the following sequence of commands will cause to set the ToS to af11 in the uplink direction, but not modify the ToS in the downlink direction:

```
ip tos af11

no ip tos downlink
```

Example

The following command sets the IP ToS to *be* with *downlink*:

```
ip tos be downlink
```

ip vlan

This command allows you to configure the VLAN identifier to be associated with the subscriber traffic in the destination context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip vlan *vlan_id*

{ default | no } ip vlan

default

Configures this command with its default setting.
Default: Disable this IP VLAN configuration. Same as **no ip vlan** command.

no

If previously configured, deletes the IP VLAN configuration in the current charging action. Whatever value is configured for the VLAN tag in the subscriber configuration or IP pool configuration (or no VLAN tag if there is no configuration elsewhere) is used.

vlan_id

Specifies the VLAN ID.
vlan_id must be an integer from 1 through 4094.

Usage

This command configures the subscriber VLAN ID which is used with the assigned address for the subscriber session to receive packets. If the IP pool from which the address is assigned is configured with a VLAN ID, then this subscriber configured VLAN ID overrides it.
Subscriber traffic can be routed to specific VLANs based on the configuration of their user profile. Using this functionality provides a mechanism for routing all traffic from a subscriber over the specified VLAN. All packets destined for the subscriber must also be sent using only IP addresses valid on the VLAN or they will be dropped.

Example

The following command sets the IP VLAN range to go up to *500*:

```
ip vlan 500
```

The following command sets the IP VLAN range back to default.

```
default ip vlan
```

nexthop-forwarding-address

This command allows you to configure the nexthop forwarding address.

Product

All

Privilege

Security Administrator, Administrator

Syntax

nexthop-forwarding-address *ipv4_address*

no nexthop-forwarding-address

no

If previously configured, deletes the nexthop-forwarding-address configuration in the current charging action.

ipv4_address

Specifies the nexthop-forwarding-address for the current charging action.
ipv4_address must be the nexthop forwarding address, and must be an IPv4 address.

Usage

Use this command to configure the nexthop-forwarding-address for a charging action. When an uplink packet matches a rule and a charging action is applied to it this nexthop forwarding address is used.
There are different methods to configure a nexthop forwarding address, they are prioritized as follows:

- The nexthop forwarding address, if configured, in a redirect ACL is used
- Else, the nexthop address configured in the charging action is used
- Else, the nexthop address, if configured, in the IP pool is used

Example

The following command sets the nexthop forwarding address for the current charging action to *10.1.1.1*:

```
nexthop-forwarding-address 10.1.1.1
```

qos-class-identifier

This command allows you to configure the QoS Class Identifier (QCI).

Product

All

Privilege

Security Administrator, Administrator

Syntax

qos-class-identifier *qos_class_identifier*

no qos-class-identifier

no

If previously configured, deletes the QCI configuration in the current charging action.

qos_class_identifier

Specifies the QCI.
qos_class_identifier must be an integer from 1 through 9 or from 128 through 254 (Operator specific).

Usage

Use this command to configure the QCI for a charging action.

Example

The following command configures the QCI as *3*:

```
qos-class-identifier 3
```

qos-renegotiate

This command allows you to configure the QoS traffic class for the Layer 7 QoS Renegotiation feature, enabling the triggering of QoS renegotiation from a rule.

Important: This command is license dependent. For more information please contact your Cisco account representative.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
qos-renegotiate traffic-class { background | conversational | interactive priority |
streaming }

no qos-renegotiate
```

no

If previously configured, deletes the qos-renegotiate traffic-class configuration in the current charging action.

background

Specifies the traffic class as Background, for traffic patterns in which the data transfer is not time-critical (for example e-mail exchange).

conversational

Specifies the traffic class as Conversational, for traffic patterns in which there is a constant flow of packets.

interactive *priority*

Specifies the traffic class as Interactive, for traffic patterns in which there is an intermittent flow of packets. *priority* specifies the traffic handling priority, and must be an integer from 1 through 3.

streaming

Specifies the traffic class as Streaming, for traffic patterns in which there is a constant flow of data in one direction, either upstream or downstream.

Usage

Use this command to configure the QoS traffic class for a charging action for the Layer 7 QoS Renegotiation feature, enabling triggering QoS renegotiation from an active-charging rule.
Layer 7 QoS Renegotiation is an extension of the Dynamic QoS Renegotiation feature. Upon matching a particular layer 7 rule, for example the access of a particular URL, the GGSN triggers the renegotiation of the PDP context.

Example

The following command sets the QoS traffic class in the charging action to streaming:

```
qos-renegotiate traffic-class streaming
```

retransmissions-counted

This command allows you to specify whether to count (for billing purposes) the number of packet retransmissions.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] retransmissions-counted
```

default

Configures this command with its default setting.
Default: Disabled; same as **no retransmissions-counted**

no

If previously enabled, disables the retransmissions-counted configuration in the current charging action.

Usage

Use this command to enable counting of the number of retransmissions.
If not enabled, retransmissions are automatically detected but discounted. The retransmissions will still be analyzed by the TCP analyzer (and higher layer analyzers), but the statistics (except for the count of retransmissions) will not be updated. Also, some higher layer analyzers (MMS, SIP, WSP, and WTP) can detect retransmissions when UDP is the transport layer.

Example

The following is an example of this command:

```
retransmissions-counted
```

service-identifier

This command allows you to configure the service identifier to use in the generated billing records, as well as the AVP used by the Credit Control Application, such as the "Service-Identifier" AVP for use by DCCA. This is a more general classifier than content-id.

Product

All

Privilege

Security Administrator, Administrator

Syntax

service-identifier *service_id*

no service-identifier

no

If previously configured, deletes the service ID configuration in the current charging action.

service_id

Specifies the service identifier.
In 12.1 and earlier releases *service_id* must be an integer from 1 through 65535.
In 12.2 and later releases, *service_id* must be an integer from 1 through 2147483647.

Usage

Use this command to configure the service identifier to use in generated billing records, as well as the AVP used by the Credit Control Application, such as the "Service-Identifier" AVP for use by DCCA. This is a more general classifier than content-id.

Example

The following command configures the service identifier in the current charging action to *99*:

```
service-identifier 99
```

tft packet-filter

This command allows you to specify the packet filter to use in TFTs sent to the MS.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] tft packet-filter *packet_filter_name*

no

If previously configured, removes the specified packet filter from the current charging action.

packet_filter_name

Specifies the packet filter to add/remove from the current charging action.
packet_filter_name must be the name of a packet filter, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the packet filter to be sent to the MS. Up to eight packet filters can be specified in a charging action.

Example

The following command configures the packet filter *filter23* to be sent to the MS:

```
tft packet-filter filter23
```

tos

This command allows you to configure the Type of Service (ToS) octets.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 |
be | ef | lower-bits tos_value } [ downlink | uplink ]

no tos [ downlink | uplink ]
```

no

Disables the ToS being used in the charging action.

af *xx*

Specifies the use of an assured forwarding *xx* Per Hop Behavior (PHB).

be

Specifies use of Best Effort forwarding PHB.

ef

Specifies use of Expedited Forwarding PHB.

lower-bits *tos_value*

Important: In 8.1 and later releases, this keyword is "**lower-bits** *tos_value*". In 8.0 release, it is *tos_value*.

Sets the least-significant 6 bits in the ToS byte with the specified numeric value. *tos_value* must be an integer from 0 through 63.

downlink

Specifies the ToS only for downlink packets.

uplink

Specifies the ToS only for uplink packets.

Usage

Use this command to set the ToS octets used in the charging action. If one of the enumerated values is set, the Differentiated Services Code Point (DSCP) bits (the six most-significant bits (MSBs) in the ToS byte) are marked. If the integer value is set, it will be written into the six least-significant bits (LSBs) of the ToS byte.

Example

The following command sets the ToS to *be* for downlink packets:

```
tos be downlink
```

tpo profile

This command allows you to specify the Traffic Performance Optimization (TPO) profile for the current charging action.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

tpo profile *tpo_profile_name*

no tpo profile

no

If previously configured, removes the TPO profile configuration from the current charging action.

tpo_profile_name

Specifies the TPO profile.
tpo_profile_name must be the name of a TPO profile, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify the TPO profile for a charging action.
When based on rule matching a charging action is selected, the TPO profile configured in it will be applied for the flow. If a TPO profile was applied to a flow through a particular charging action, and subsequently a different charging action that does not have a TPO profile configured in it is applied to the same flow, TPO will not be disabled.

Example

The following command configures a TPO profile named *tpoprofile10* for the current charging action:

```
tpo profile tpoprofile10
```

video bitrate

This command allows you to specify the default target bit rate to use for the video pacing feature on the Mobile Video Gateway. This value is also used as the suggested maximum bit rate for the video optimization policy control feature and the dynamic inline transrating feature.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

[default | no] video bitrate *bit_rate* **[-noconfirm]**

default

Sets video bitrate to its default value.

no

Deletes the video bit rate if previously configured.

video bitrate *bit_rate*

Specifies the bit rate, in bits per second, at which the TCP video flow should be paced during video pacing. This value is also used as the suggested maximum bit rate for the video optimization policy control feature and the dynamic inline transrating feature. For video pacing, this default bit rate is used on each video flow until the rate determination function calculates the optimal bit rate for pacing.
bit_rate must be an integer from 0 to 256000000.
Default: 0

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to specify the default bit rate to use for the video pacing feature, and the suggested maximum bit rate for the video optimization policy control feature and the dynamic inline transrating feature.

Example

The following command sets the bit rate for the video flow at *300000* (300kbps):

```
video bitrate 300000
```

video cae-readdressing

This command allows you to enable CAE (Content Adaptation Engine) re-addressing, allowing video traffic to be fetched from the CAEs in the CAE group. The CAE is an optional component of the Mobile Videoscape.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

`[ no ] video cae-readdressing [ xheader-format` *`xheader_format_name`* **`]`**

`no`

Disables CAE re-addressing if previously configured.

`video cae-readdressing`

Enables CAE re-addressing, allowing video traffic to be fetched from the CAEs in the CAE group.

`xheader-format` *`xheader_format_name`*

Specifies an HTTP x-header (Extension header) format for readdressing. When specified, the MVG inserts a destination IP address and TCP port number in a proprietary HTTP x-header in the HTTP request to the CAE. The CAE uses this information to connect to the OS (Origin Server) to retrieve selected video clips for adaptation.
`xheader_format_name` must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to enable CAE re-addressing on the Mobile Video Gateway.

Example

The following command enables CAE re-addressing:

```
video cae-readdressing xheader-format format_1
```

video detailed-statistics

This command allows you to enable the collection of detailed video statistics.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] video detailed-statistics [ -noconfirm ]
```

default

Sets video detailed-statistics to its default value, which is the same as **[no]**.

no

Disables the video statistics feature if previously enabled.

video detailed-statistics

Enables the video statistics feature. When a flow matches a rule definition for video during DPI (Deep Packet Inspection), the video statistics feature begins collecting detailed statistics for the video flow.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to enable the video statistics feature.

Example

The following command enables the video statistics feature:

```
video detailed-statistics
```

video optimization-preprocessing all

This command allows you to enable CAE re-addressing by enabling the Active Charging Service (ACS) to re-address video requests to the CAEs in the CAE group and enables transrating by enabling the ACS to transrate video requests.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] video optimization-preprocessing all
```

no

Disables CAE re-addressing and transrating if currently enabled.

video optimization-preprocessing cae-readdressing

Enables CAE re-addressing by enabling the ACS to re-address video requests to the CAEs in the CAE group and enables transrating by enabling the ACS to transrate video requests.

Usage

Use this command to enable CAE re-addressing by enabling the ACS to re-address video requests to the CAEs in the CAE group and enable transrating by enabling the ACS to transrate video requests.

Example

The following command enables CAE re-addressing and transrating:

```
video optimization-preprocessing all
```

video optimization-preprocessing cae-readdressing

This command allows you to enable CAE re-addressing by enabling the Active Charging Service (ACS) to re-address video requests to the CAEs in the CAE group.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] video optimization-preprocessing cae-readdressing
```

no

Disables CAE re-addressing if currently enabled.

video optimization-preprocessing cae-readdressing

Enables CAE re-addressing by enabling the ACS to re-address video requests to the CAEs in the CAE group.

Usage

Use this command to enable CAE re-addressing by enabling the ACS to re-address video requests to the CAEs in the CAE group.

Example

The following command enables CAE re-addressing:

```
video optimization-preprocessing cae-readdressing
```

video optimization-preprocessing transrating

This command allows you to enable video transrating by enabling the Active Charging Service (ACS) to transrate video requests.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] video optimization-preprocessing transrating
```

no

Disables transrating if currently enabled.

video optimization-preprocessing transrating

Enables video transrating by enabling ACS to transrate video requests.

Usage

Use this command to enable video transrating by enabling the ACS to transrate video requests.

Example

The following command enables video transrating:

```
video optimization-preprocessing transrating
```

video pacing by-policing

This command allows you to enable the video pacing feature.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

[default | no] video pacing by-policing [initial-burst-duration *value* **| normal-burst-duration** *value* **][-noconfirm]**

default

Sets video pacing by-policing to its default value, which is the same as **[no]**.

no

Deletes the video pacing by-policing settings and disables video pacing if previously configured.

video pacing by-policing

Enables the video pacing feature. When enabled, video pacing is applied per TCP video flow. The command syntax **by-policing** enables pacing enforcement by the policing method, which is the available method for this software release.

initial-burst-duration *value*

Specifies the duration, in seconds, for the allowed initial burst of video content. Note that the initial burst is configured in terms of time, so that for video files with different encoding bit rates, the amount of bytes allowed without enforcing pacing gets adjusted accordingly. The amount of bytes allowed is calculated by (video encoding rate * initial-burst-duration).
value must be an integer between 1 and 30.
Default: 10 seconds

normal-burst-duration *value*

Specifies the duration, in seconds, for the allowed normal burst of video content after the initial burst is completed. Like the initial burst, the normal burst is also configured in terms of time, so that for video files with different encoding bit rates, the amount of bytes allowed without enforcing pacing gets adjusted accordingly. The amount of bytes allowed is calculated by (video encoding rate * normal-burst-duration).
value must be an integer between 1 and 30.
Default: 3 seconds

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to enable video pacing by policing.

Example

The following command enables video pacing by policing with an initial burst duration of 15 seconds and a normal burst duration of 3 seconds:

```
video pacing by-policing initial-burst-duration 15 normal-burst-duration
3
```

video transrating target-rate-reduction

This command allows you to specify the target bit rate reduction for dynamic inline transrating.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

video transrating target-rate-reduction *percentage_of_input_rate*

video transrating target-rate-reduction *percentage_of_input_rate*

This command configures transrating by specifying the target bit rate reduction as a percentage of the input bit rate, which can be between 1 and 50 percent.

Usage

Use this command to configure the target bit rate reduction for dynamic inline transrating.

Example

The following command specifies the target bit rate reduction as 20 percent of the input bit rate:

```
video transrating target-rate-reduction 20
```

xheader-insert

This command allows you to specify the extension-header (x-header) format whose fields have to be inserted in HTTP GET and POST request packets.

Important: This command is license dependent. For more information please contact your Cisco account representative.

Product

All

Privilege

Security Administrator, Administrator

Syntax

xheader-insert xheader-format *xheader_format_name* **[encryption rc4md5 [encrypted] key** *key* **] [first-request-only] [-noconfirm]**

no xheader-insert

no

Removes previously configured x-header format name.

xheader-format *xheader_format_name*

Enables x-header mode configuration, and specifies the x-header format whose fields are to be inserted in the packets.
xheader_format_name must be the name of an x-header format, and must be an alphanumeric string of 1 through 63 characters.

encryption rc4md5 [encrypted] key *key*

If the x-header format has any encrypted fields defined, specifies to use RC4MD5 encryption.
After configuring this option, the fields in xheader format having “encrypt” enabled will be encrypted as follows:

1. The MD5 hash of the configure key will be calculated.
2. This MD5 hash will be used as a key for RC4 encryption.
3. This encrypted value will be base64 encoded to get the final X-header value. The final inserted X-header will be X-alias: base64(RC4(MD5(key),MSISDN)).

In the default case, if encryption is not enabled as above, the plain text value of the xheader field will be inserted.
Note that if the value of the key is changed on the fly, it will take effect only in case of new calls. Also, if the per rulebase RSA encryption is also enabled in the same config, per charging-action RC4MD5 encryption will take precedence over it.
key specifies the key as an alphanumeric string of 8 through 15 characters.
encryption specifies use of encryption.
The *key* can be configured either as plain text or encrypted. However, in the output of the **show configuration** command it will always be displayed as encrypted. And, in the output of the **show configuration showsecrets** command it will be displayed as plain text.

first-request-only

Specifies x-header insertion only for the first HTTP request in the IP flow. If not configured, the default behavior is insertion for all requests.

-noconfirm

Specifies that the command must execute without any prompts and confirmation from the user.

Usage

Use this command to enable x-header mode, and specify the x-header format name whose fields are to be inserted in HTTP GET and POST request packets.
Also, see the **xheader-format** command in the *ACS Configuration Mode Commands* and *ACS X-header Format Configuration Mode Commands* chapters.

Example

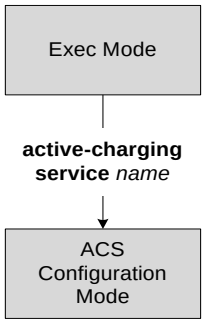
The following command enables x-header mode, and specifies the x-header format name as *test12*:

```
xheader-insert xheader-format test12
```

Chapter 8
ACS Configuration Mode Commands

The ACS Configuration Mode is used to manage active charging service (ACS)/enhanced charging service (ECS) configurations. ACS provides flexible, differentiated, and detailed billing to subscribers through Layer 3 through Layer 7 packet inspection and the ability to integrate with back-end billing mediation systems.

Important: In this release only one active charging service can be configured in a system.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

access-ruledef

This command allows you to create/configure/delete access rule definitions (ruledefs).

Important: This command is available only in StarOS 8.1 and in StarOS 9.0 and later releases, and must be used to configure the Policy-based Stateful Firewall and NAT features.

Product

NAT, FW

Privilege

Security Administrator, Administrator

Syntax

access-ruledef *access_ruledef_name* **[-noconfirm]**

no access-ruledef *access_ruledef_name*

no

If previously configured, deletes the specified access ruledef.

access_ruledef_name

Specifies the access ruledef to add/configure/delete.
access_ruledef_name must be the name of an access ruledef, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters.
If the named access ruledef does not exist, it is created, and the CLI mode changes to the Firewall-and-NAT Access Ruledef Configuration Mode wherein the ruledef can be configured.
If the named access ruledef already exists, the CLI mode changes to the Firewall-and-NAT Access Ruledef Configuration Mode for that access ruledef.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete an access ruledef. A ruledef contains different conditions/criteria to permit, drop, or reject a packet/connection/traffic based on one or more parameters. The ruledef name must be unique within the service. Host pool, port map, IMSI pool, and access/firewall, routing, and charging ruledefs configured in the active charging service must all have unique names.

Important: An access ruledef can be referenced by multiple Stateful Firewall rulebases.

Important: Access ruledefs are different from ACS ruledefs.

Also see the *Firewall-and-NAT Access Ruledef Configuration Mode Commands* chapter.

Example

The following command creates an access ruledef named *ruledef1*, and enters the Firewall-and-NAT Access Ruledef Configuration Mode:

```
access-ruledef ruledef1
```

bandwidth-policy

This command allows you to create/configure/delete bandwidth policies.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

bandwidth-policy *bandwidth_policy_name* **[-noconfirm]**

no bandwidth-policy *bandwidth_policy_name*

no

If previously configured, deletes the specified bandwidth policy from the active charging service.

bandwidth_policy_name

Specifies the bandwidth policy to add/configure/delete.
bandwidth_policy_name must be the name of a bandwidth policy, and must be an alphanumeric string of 1 through 63 characters.
If the named bandwidth policy does not exist, it is created, and the CLI mode changes to the ACS Bandwidth Policy Configuration Mode wherein the bandwidth policy can be configured.
If the named bandwidth policy already exists, the CLI mode changes to the ACS Bandwidth Policy Configuration Mode for that bandwidth policy.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete a bandwidth policy.
Also see the *ACS Bandwidth Policy Configuration Mode Commands* chapter.

Example

The following command creates a bandwidth policy named *test73*, and enters the ACS Bandwidth Policy Configuration Mode:

```
bandwidth-policy test73
```

buffering-limit

This command allows you to configure packet buffering limits.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

buffering-limit { flow-max-packets *flow_max_packets* **| subscriber-max-packets** *subscriber_max_packets* **}**

{ default | no } buffering-limit { flow-max-packets | subscriber-max-packets }

default

Configures this command with its default setting.
Default: No limit, other than the maximum amount of available memory.

no

Disables the buffering limit configuration.

flow-max-packets *flow_max_packets*

Specifies the maximum number of packets that can be buffered per flow.
flow_max_packets must be an integer from 1 through 255.

subscriber-max-packets *subscriber_max_packets*

Specifies the maximum number of packets that can be buffered per subscriber.
subscriber_max_packets must be an integer from 1 through 255.

Usage

Use this command to configure the limits for buffering packets sent by a subscriber, while waiting for a response from the Diameter server. Packets need to be buffered for various reasons, such as, waiting for Credit Control Authorization or waiting for the result of a content filtering rating request.

Example

The following command sets the buffering limit per flow to *55*:

```
buffering-limit flow-max-packets 55
```

charging-action

This command allows you to create/configure/delete ACS charging actions.

Important: A maximum of 2048 charging actions can be configured in the active charging service.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] charging-action` *`charging_action_name`* **`[ -noconfirm ]`**

`no`

If previously configured, deletes the specified charging action from the active charging service.

`charging_action_name`

Specifies the charging action to add/configure/delete.
`charging_action_name` must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters and can contain punctuation characters.
If the named charging action does not exist, it is created, and the CLI mode changes to the ACS Charging Action Configuration Mode wherein the charging action can be configured.
If the named charging action already exists, the CLI mode changes to the ACS Charging Action Configuration Mode for that charging action.
The charging action's name must be unique in the active charging service. Up to 2048 charging actions can be configured in the active charging service.

`-noconfirm`

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete an ACS charging action.
A charging action represents actions to be taken when a configured rule is matched. Actions could range from generating an accounting record (for example, an EDR) to dropping the IP packet, etc. The charging action will also determine the metering principle—whether to count retransmitted packets and which protocol field to use for billing (L3/L4/L7 etc).
Also see the *ACS Charging Action Configuration Mode Commands* chapter.

Example

The following command creates a charging action named *`action123`* and changes to the ACS Charging Action Configuration Mode:

```
charging-action action123
```

content-filtering category match-method

This command allows you to specify the match method to look up URLs in the Category-based Content Filtering database.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

```
content-filtering category match-method { exact | generic }

default content-filtering category match-method
```

default

Configures this command with its default setting.
Default: **generic**

exact

Specifies the exact-match method, wherein URLs are rated only on exact match with URLs present in the Category-based Content Filtering database.

generic

Specifies the generic match method, wherein normalization, multi-lookups, and rollback algorithms are applied to URLs during look up. URLs are rated on generic match with URLs present in the Category-based Content Filtering database.

Usage

Use this command to set the match method to look up URLs in the Category-based Content Filtering database.

Example

The following command sets the exact-match method to look up URLs in the Category-based Content Filtering database:

```
content-filtering category match-method exact
```

content-filtering category policy-id

This command allows you to create/configure/delete Content Filtering Category Policies for Category-based Content Filtering support.

Important: A maximum of 64 Content Filtering Category Policies can be configured in the active charging service.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

content-filtering category policy-id *cf_policy_id* **[description [** *description_string* **]] [-noconfirm]**

no content-filtering category policy-id *cf_policy_id*

no

If previously configured, deletes the specified Content Filtering Category Policy from the active charging service.

cf_policy_id

Specifies the Content Filtering Category Policy ID to add/configure/delete.
cf_policy_id must be an integer from 1 through 4294967295.
If the specified policy ID does not exist, it is created and the CLI mode changes to the Content Filtering Policy Configuration Mode, wherein the policy can be configured.
If the specified policy ID already exists, the CLI mode changes to the Content Filtering Policy Configuration Mode for that policy.

description [*description_string* **]**

Specifies a description for the Content Filtering Category Policy.
description_string must be an alphanumeric string of 1 through 31 characters.
Note that both **description** and *description_string* are optional.
"**description** *description_string*" saves *description_string* as the new description.
"**description**" removes the previously specified description.
This description is displayed in the output of the "**show content-filtering category policy-id id** *id*" and "**show active-charging service name** *service_name*" commands.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete a Content Filtering Category Policy.

Also see the *Content Filtering Policy Configuration Mode Commands* chapter.

Example

The following command creates a Content Filtering Policy with the ID *101*, and enters the Content Filtering Policy Configuration Mode:

```
content-filtering category policy-id 101
```

credit-control

This command allows you to enable/disable Prepaid Credit Control Configuration Mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] credit-control [group *cc_group_name* **]**

no

Disables the specified Prepaid Credit Control Application configuration.

group *cc_group_name*

Important: This option is only available in StarOS 8.1 and later releases.

Specifies the credit control group to add/configure/delete.
cc_group_name must be the name of a credit control group, and must be an alphanumeric string of 1 through 63 characters.
If the named credit control group does not exist, it is created, and the CLI mode changes to the Credit Control Configuration Mode, wherein the credit control group can be configured.
If the named credit control group already exists, the CLI mode changes to the Credit Control Configuration Mode for that credit control group.
Creating different credit control groups enables applying different credit control configurations (DCCA dictionary, failure-handling, session-failover, Diameter endpoint selection, etc.) to different subscribers on the same system.
Without credit control groups, only one credit control configuration is possible on a system. All the subscribers in the system will have to use the same configuration.

Usage

Use this command to enable/disable Prepaid Credit Control Configuration for RADIUS/Diameter charging mode.
Also see the *Credit Control Configuration Mode Commands* chapter.

Example

The following command enables prepaid credit control accounting to use RADIUS and/or Diameter interface mode.

```
credit-control
```

diameter credit-control

Description This command has been deprecated, and is replaced by the credit-control command.

edr-format

This command allows you to create/configure/delete ACS Event Data Record (EDR) formats.

Product

All

Privilege

Security Administrator, Administrator

Syntax

edr-format *edr_format_name* **[-noconfirm]**

no edr-format *edr_format_name*

no

If previously configured, deletes the specified EDR format from the active charging service.

edr_format_name

Specifies the EDR format to add/configure/delete.
edr_format_name must be a string of 1 through 63 characters.
If the named EDR format does not exist, it is created, and the CLI mode changes to the EDR Format Configuration Mode wherein the EDR format can be configured.
If the named EDR format already exists, the CLI mode changes to the EDR Format Configuration Mode for that EDR format.
The EDR format name must be unique in the active charging service. Up to 256 combined total EDR plus User Data Record (UDR) formats can be configured in the active charging service.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete an EDR format.
Also see the *EDR Format Configuration Mode Commands* chapter.

Example

The following command creates an EDR format named *edr_format1*:

```
edr-format edr_format1
```

edr-udr-flow-control

This command allows you to enable/disable flow control between Session Managers (SessMgrs) and the CDRMOD process.

Product

All

Privilege

Security Administrator, Administrator

Syntax

edr-udr-flow-control [unsent-queue-size *unsent_queue_size* **]**

{ default | no } edr-udr-flow-control

no

If previously enabled, disables the flow control configuration.

default

Configures this command with its default setting.
Default: Flow control is enabled; **unsent-queue-size**: 375

unsent-queue-size *unsent_queue_size*

Specifies the flow control unsent queue size at Session Manager (SessMgr) level.
unsent_queue_size must be an integer from 1 through 2500.

Usage

Use this command to enable Flow Control between SessMgr and the CDRMOD process, and configure the unsent queue size.

Example

The following command enable Flow Control between SessMgrs and the CDRMOD process, and configure the unsent queue size to *1000*:

```
edr-udr-flow-control unsent-queue-size 1000
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

fair-usage deact-margin

This command allows you to configure the deactivate margin for the Fair Usage feature.

Product

ACS, ADC, CF, FW, NAT

Privilege

Security Administrator, Administrator

Syntax

fair-usage deact-margin *deactivate_margin*

default fair-usage deact-margin

default

Configures this command with its default setting.
Default: 5 percent

deactivate_margin

Specifies that Fair Usage monitoring must be disabled when the instance-level credit usage goes *deactivate_margin* percentage below *usage_threshold*.
deactivate_margin is a percentage value, and must be an integer from 1 through 100.

Usage

Use this command to configure when to disable the Fair Usage feature, which enables SessMgr instance-level load balancing for in-line service features, and resource usage control for subscribers. For additional information, refer to the feature description in the *Enhanced Charging Service Administration Guide*.

Example

The following command configures the deactivate margin to disable Fair Usage monitoring to 10% below the session resource usage threshold (65%):

```
fair-usage deact-margin 10
```

fair-usage tcp-proxy

This command allows you to configure the maximum number of flows for which TCP Proxy can be used per subscriber, and what portion of ECS memory should be reserved for TCP Proxy flows.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

fair-usage tcp-proxy { max-flows-per-subscriber *max_flows_subscriber* **| memory-share** *memory_share* **}**

max-flows-per-subscriber *max_flows_subscriber*

Specifies the maximum number of flows for which TCP Proxy can be used per subscriber.
This limit is per Session Manager.
max_flows_subscriber must be an integer from 1 through 1000.
Default: 5

memory-share *memory_share*

Specifies what portion of ECS memory should be reserved for TCP Proxy flows.
memory_share is a percentage value, and must be an integer from 1 through 100.
Default: 10%

Usage

Use this command to configure the maximum number of flows for which TCP Proxy can be used for a subscriber, and what portion of ECS memory should be reserved for TCP Proxy flows.

Example

The following command configures 100 as the maximum number of flows for which TCP Proxy can be enabled for the subscriber:

```
fair-usage tcp-proxy max-flows-per-subscriber 100
```

fair-usage threshold-percent

This command allows you to configure the usage threshold to start Fair Usage monitoring.

Product

ACS, ADC, CF, FW, NAT

Privilege

Security Administrator, Administrator

Syntax

fair-usage threshold-percent *usage_threshold*

default fair-usage threshold-percent

default

Configures this command with its default setting.
Default: 50 percent

usage_threshold

Specifies the threshold to start Fair Usage monitoring. Until the credit usage hits this threshold, all session resource allocation is allowed. On crossing this threshold, any new resource allocation request is evaluated before being allowed or denied.
usage_threshold is a percentage value, and must be an integer from 1 through 100.

Usage

Use this command to configure the threshold to enable the Fair Usage feature, which enables SessMgr instance-level load balancing for in-line service features, and resource usage control for subscribers. For additional information, refer to the feature description in the *Enhanced Charging Service Administration Guide*.

Example

The following command enables the Fair Usage feature, and configures the session resource usage threshold to start Fair Usage monitoring to 75%:

```
fair-usage threshold-percent 75
```

firewall flow-recovery

This command allows you to configure the Stateful Firewall's Flow Recovery feature.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
firewall flow-recovery { { downlink [ [ timeout timeout ] [ no-flow-creation ] + ] } | { uplink [ timeout timeout ] } }

{ default | no } firewall flow-recovery { downlink | uplink }
```

default

Configures this command with its default setting.
Default: Downlink and uplink flow recovery enabled, 300 seconds

no

Disables the flow recovery configuration.

downlink | uplink

Specifies the packets:

- **downlink**: Enables flow recovery for packets from the downlink direction.
- **uplink**: Enables flow recovery for packets from the uplink direction.

timeout *timeout*

Specifies the Stateful Firewall Flow Recovery Timeout setting, in seconds.
timeout must be an integer from 1 through 86400.
Default: 300 seconds

no-flow-creation

Specifies not to create data session/flow-related information for downlink-initiated packets (from the Internet to the subscriber) while the firewall downlink flow-recovery timer is running, but send to subscriber.

Usage

Use this command to configure Stateful Firewall Flow Recovery feature.

Important: NAT flows will not be recovered.

Example

The following command configures Stateful Firewall Flow Recovery for packets in downlink direction with a timeout setting of *600* seconds:

```
firewall flow-recovery downlink timeout 600
```

firewall max-ip-packet-size

Description In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the ACS Rulebase Configuration Mode.

firewall mime-flood

Description In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the ACS Rulebase Configuration Mode.

firewall nat-alg

This command enables/disables Network Address Translation (NAT) Application Level Gateways (ALGs).

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

`[ default | no ] firewall nat-alg { all | ftp | h323 | pptp | rtsp | sip } [ ipv4-and-ipv6 | ipv4-only | ipv6-only ]`

`default`

Configures this command with the default setting for the specified parameter.
Default:

- **`ftp`**: Enabled
- **`h323`**: Enabled
- **`pptp`**: Disabled
- **`rtsp`**: Disabled
- **`sip`**: Disabled

`no`

Disables all/ or the specified NAT ALG configuration. When disabled, the ALG(s) will not do any payload translation for NATd calls.

`all | ftp | h323 | pptp | rtsp | sip`

Specifies the NAT ALG to enable/disable.

- **`all`**: Enables/disables all of the following NAT ALGs.
- **`ftp`**: Enables/disables File Transfer Protocol (FTP) NAT ALG.
- **`h323`**: Enables/disables H323 NAT ALG.
- **`pptp`**: Enables/disables Point-to-Point Tunneling Protocol (PPTP) NAT ALG.
- **`rtsp`**: Enables/disables Real Time Streaming Protocol (RTSP) ALG.
- **`sip`**: Enables/disables Session Initiation Protocol (SIP) NAT ALG.

`ipv4-and-ipv6 | ipv4-only | ipv6-only`

Specifies to enable/disable NAT44/NAT64 ALG.

- **`ipv4-and-ipv6`**: Enables both NAT44 and NAT64 ALGs.
- **`ipv4-only`**: Enables only NAT44 ALG.
- **`ipv6-only`**: Enables only NAT64 ALG.

Usage

Use this command to enable/disable NAT ALGs.
To enable NAT ALG processing, in addition to this configuration, ensure that the routing rule for that particular protocol is added in the rulebase.

Example

The following command enables FTP NAT ALG:

```
firewall nat-alg ftp
```

The following command disables FTP NAT ALG:

```
no firewall nat-alg ftp
```

The following command enables FTP NAT ALG, and disables H.323, PPTP, RTSP, and SIP NAT ALGs:

```
default firewall nat-alg all
```

firewall no-ruledef-matches

Description In StarOS 8.1 and later releases, this command is available in the ACS Rulebase Configuration Mode.

firewall port-scan

This command allows you to configure Stateful Firewall's Port Scan Detection algorithm.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall port-scan { connection-attempt-success-percentage { non-scanner | scanner } *percentage* | inactivity-timeout *inactivity_timeout* | protocol { tcp | udp } response-timeout *response_timeout* | scanner-policy { block inactivity-timeout *inactivity_timeout* | log-only } }

default firewall port-scan { connection-attempt-success- percentage { non-scanner | scanner } | inactivity-timeout | protocol { tcp | udp } response-timeout | scanner-policy }

---

default

Configures this command with its default setting.

---

connection-attempt-success-percentage { non-scanner | scanner } *percentage*

Specifies the connection attempt success percentage:

- **non-scanner**: Specifies the connection attempt success percentage for a non-scanner.

  percentage must be an integer from 60 through 99.

  Default: 70%

- **scanner**: Specifies the connection attempt success percentage for a scanner.

  percentage must be an integer from 1 through 40.

  Default: 30%

---

inactivity-timeout *inactivity_timeout*

Specifies the port scan inactivity timeout period, in seconds.
inactivity_timeout must be an integer from 60 through 1800.
Default: 300 seconds

---

protocol { tcp | udp } response-timeout *response_timeout*

Specifies transport protocol and response-timeout period:

- **tcp**: Specifies response timeout for TCP.

  response_timeout must be an integer from 3 through 30.

- **udp**: Specifies response timeout for UDP.

  response_timeout must be an integer from 3 through 60.

Default: 3 seconds

scanner-policy { block inactivity-timeout *inactivity_timeout* **| log-only }**

Specifies how to treat packets from a source address that has been detected as a scanner:

- **block inactivity-timeout** *inactivity_timeout*: Specifies blocking any subsequent traffic from the scanner. If the scanner is found to be inactive for the inactivity-timeout period, then the scanner is no longer blocked, and traffic is allowed.

  inactivity_timeout specifies the scanner inactivity timeout period, in seconds, and must be an integer from 1 through 4294967295.

- **log-only**: Specifies logging scanner information without blocking scanner traffic.

Default: **log-only**

Usage

Use this command to configure the Stateful Firewall Port Scan Detection algorithm enabled by the **firewall dos-protection port-scan** CLI command.
This protection tracks all uplink source addresses, and the packets they initiate towards all subscribers that have this protection enabled.

Example

The following command configures the Stateful Firewall Port Scan inactivity timeout setting to *900* seconds:

```
firewall port-scan inactivity-timeout 900
```

firewall ruledef

This command allows you to create/configure/delete Stateful Firewall ruledefs.

Important: This command is available only in StarOS 8.1. This command must be used to configure the Rulebase-based Stateful Firewall and NAT features.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall ruledef *firewall_ruledef_name* **[-noconfirm]**

no firewall ruledef *firewall_ruledef_name*

no

If previously configured, deletes the specified Stateful Firewall ruledef from the active charging service.

firewall_ruledef_name

Specifies the Stateful Firewall ruledef to add/configure/delete.
firewall_ruledef_name must be the name of a Stateful Firewall ruledef, and must be a string of 1 through 63 characters, and can contain punctuation characters.
If the named ruledef does not exist, it is created, and the CLI mode changes to the Firewall Ruledef Configuration Mode wherein the ruledef can be configured.
If the named Stateful Firewall ruledef already exists, the CLI mode changes to the Firewall Ruledef Configuration Mode for that ruledef.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete a Stateful Firewall ruledef. A Stateful Firewall ruledef contains different conditions to permit, drop, or reject a packet/connection/traffic based on one or more parameters.
The ruledef name must be unique with in the active charging service. Host pool, port map, IMSI pool, and Stateful Firewall, routing, and charging ruledefs must have unique names.
A Stateful Firewall ruledef can be referenced by multiple Stateful Firewall rulebases.

Important: The Stateful Firewall ruledefs are different from the ACS ruledefs.

Also see the *Firewall-and-NAT Access Ruledef Configuration Mode Commands* chapter.

Example

The following command creates a Stateful Firewall ruledef named *fw_ruledef1*, and enters the Firewall Ruledef Configuration Mode:

```
firewall ruledef fw_ruledef1
```

firewall tcp-syn-flood-intercept

Description In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the ACS Rulebase Configuration Mode.

firewall track-list

This command allows you to configure the maximum number of server IP addresses to be tracked that are involved in any kind of denial-of-service (DoS) attacks.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall track-list attacking-servers *no_of_servers*

{ default | no } firewall track-list attacking-servers

default

Configures this command with its default setting.
Default: 10 servers

no

Important: This command variant is available only in StarOS 8.3 and later releases.

If previously configured, deletes the configuration from the active charging service.

attacking-servers *no_of_servers*

Specifies the maximum number of servers to track.
no_of_servers must be an integer from 1 through 100.

Usage

Use this command to configure the maximum number of server IP addresses to be tracked that are involved in any kind of DoS attacks.

Example

The following command configures the maximum number of server IP addresses to be tracked that are involved in any kind of DoS attacks to *20*:

```
firewall track-list attacking-servers 20
```

fw-and-nat action

This command allows you to create/configure/delete Firewall-and-NAT actions.

Important: This command is available only in 11.0 and later releases. This command must be used to configure the Stateful Firewall and NAT Action.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

fw-and-nat action *action_name* **[-noconfirm]**

no fw-and-nat action *action_name*

no

If previously configured, deletes the specified Firewall-and-NAT action from the active charging service.

action_name

Specifies the Firewall-and-NAT action to add/configure/delete.
action_name must be the name of a Firewall-and-NAT action, and must be an alphanumeric string of 1 through 63 characters.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete a Firewall-and-NAT action.
Entering this command results in the following prompt:
`[context_name]hostname(config-fw-and-nat-action)#`
Also see the *Firewall-and-NAT Action Configuration Mode Commands* chapter.

Example

The following command creates a Firewall-and-NAT action named *test1*, and changes to the Firewall-and-NAT Action Configuration Mode:

```
fw-and-nat action test1
```

fw-and-nat policy

This command allows you to create/configure/delete Firewall-and-NAT policies.

Important: This command is available only in StarOS 8.1 and in StarOS 9.0 and later releases. This command must be used to configure the Policy-based Stateful Firewall and NAT features.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

fw-and-nat policy *policy_name* **[-noconfirm]**

no fw-and-nat policy *policy_name*

no

If previously configured, deletes the specified Firewall-and-NAT policy from the active charging service.

Important: When a Firewall-and-NAT policy is deleted, for all subscribers using the policy, Stateful Firewall and NAT processing is disabled, also ACS sessions for the subscribers are dropped. In case of session recovery, the calls are recovered but with Stateful Firewall and NAT disabled.

policy_name

Specifies the Firewall-and-NAT policy to add/configure/delete.
policy_name must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete a Firewall-and-NAT policy.
Entering this command results in the following prompt:
`[context_name]hostname(config-fw-and-nat-policy)#`
Also see the *Firewall-and-NAT Policy Configuration Mode Commands* chapter.

Example

The following command creates a Firewall-and-NAT policy named *test321*, and changes to the Firewall-and-NAT Policy Configuration Mode:

```
fw-and-nat policy test321
```

group-of-objects

This command allows you to create/configure/delete an ACS group-of-objects.

Important: This command is available only in StarOS 10.2 and later releases.

Important: A maximum of 16 object groups can be configured in the active charging service. And a maximum of 128 objects can be configured within each object group.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

group-of-objects *objects_group_name* **[type string [-noconfirm]]**

no group-of-objects *objects_group_name*

no

If previously configured, deletes the specified group-of-objects from the active charging service.

objects_group_name

Specifies the group-of-objects to add/configure/delete.
objects_group_name must be the name of a group-of-objects, and must be an alphanumeric string of 1 through 63 characters.
If the named group-of-objects does not exist, it is created, and the CLI mode changes to the ACS Group-of-Objects Configuration Mode wherein the group can be configured.
If the named group-of-objects already exists, the CLI mode changes to the ACS Group-of-Objects Configuration Mode for that group.

type

Specifies the data type for the group-of-objects.

Important: "string" is the only data type supported in this release.

string

Specifies the data type as string.
When creating a group, specifying the data type is mandatory.
When modifying an existing group, specifying the data type is optional.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete a group-of-objects.
Also see the *ACS Group-of-Objects Configuration Mode Commands* chapter.

Example

The following command creates a group-of-objects named *test4* with the data type string, and enters the ACS Group-of-Objects Configuration Mode:

```
group-of-objects test4 type string
```

group-of-prefixed-urls

This command allows you to create/configure/delete an ACS group-of-prefixed-URLs.

Important: This command is customer specific. For more information contact your Cisco account representative.

Important: A maximum of 64 group-of-prefixed-URL groups can be configured in the active charging service.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

group-of-prefixed-urls *prefixed_urls_group_name* **[-noconfirm]**

no group-of-prefixed-urls *prefixed_urls_group_name*

no

If previously configured, deletes the specified group-of-prefixed-urls from the active charging service.

prefixed_urls_group_name

Specifies the group-of-prefixed-urls to add/configure/delete.
prefixed_urls_group_name must be the name of a group-of-prefixed-urls, and must be an alphanumeric string of 1 through 63 characters.
If the named group-of-prefixed-urls does not exist, it is created, and the CLI mode changes to the ACS Group-of-Prefixed-URLs Configuration Mode wherein the group can be configured.
If the named group-of-prefixed-urls already exists, the CLI mode changes to the ACS Group-of-Prefixed-URLs Configuration Mode for that group.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete a group-of-prefixed-URLs.
Also see the *ACS Group-of-Prefixed-URLs Configuration Mode Commands* chapter.

Example

The following command creates group-of-prefixed-urls named *test5*, and enters the ACS Group-of-Prefixed-URLs Configuration Mode:

```
group-of-prefixed-urls test5
```

group-of-ruledefs

This command allows you to create/configure/delete an ACS group-of-ruledefs.

Important: A maximum of 64 groups-of-ruledefs can be configured in the active charging service.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

group-of-ruledefs *ruledefs_group_name* **[-noconfirm]**

no group-of-ruledefs *ruledefs_group_name*

no

If previously configured, deletes the specified group-of-ruledefs from the active charging service.

ruledefs_group_name

Specifies the group-of-ruledefs to add/configure/delete.
ruledefs_group_name must be unique within the active charging service, and must be a string of 1 through 63 characters. Up 64 groups may be configured.
If the named group-of-ruledefs does not exist, it is created, and the CLI mode changes to the ACS Group-of-Ruledefs Configuration Mode wherein the group can be configured.
If the named group-of-ruledefs already exists, the CLI mode changes to the ACS Group-of-Ruledefs Configuration Mode for that group.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete a group-of-ruledefs.
A group-of-ruledefs is a collection of rule definitions to use in access policy creation. The group-of-ruledefs name must be unique within the service.
Also see the *ACS Group-of-Ruledefs Configuration Mode Commands* chapter.

Example

The following command creates a group-of-ruledefs named *group1*, and enters the ACS Group-of-Ruledefs Configuration Mode:

```
group-of-ruledefs group1
```

h323 time-to-live

This command allows you to configure the time period for which an endpoint's registration to an H.323 gatekeeper is valid.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

h323 time-to-live *timeout*

default h323 time-to-live

default

Configures this command with its default setting.
Default: 3600 seconds

timeout

Specifies the timeout setting, in seconds.
timeout must be an integer from 1 through 2147483647.

Usage

Use this command to configure the time period for which an endpoint's registration to a gatekeeper is valid.

Example

The following command configures the time for an endpoint registration with a timeout setting of *5* seconds:

```
h323 time-to-live 5
```

h323 timeout

This command allows you to configure the timeout intervals for various H.323 requests.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

h323 timeout { admission *admission_timeout* **| discovery** *discovery_timeout* **| location** *location_timeout* **| registration** *registration_timeout* **| unregistration** *unregistration_timeout* **}**

default h323 timeout { admission | discovery | location | registration | unregistration }

default

Configures this command with the default setting for the specified parameters.

admission *admission_timeout*

Configures the timeout value for the admission request sent to the gatekeeper.
admission_timeout must be an integer from 1 through 20.
Default: 10 seconds

discovery *discovery_timeout*

Configures the timeout value for the gatekeeper request message sent to the Gatekeeper.
discovery_timeout must be an integer from 1 through 20.
Default: 10 seconds

location *location_timeout*

Configures the timeout value for the location request message sent to the Gatekeeper.
location_timeout must be an integer from 1 through 20.
Default: 10 seconds

registration *registration_timeout*

Configures the timeout value for the registration request message sent to the Gatekeeper.
registration_timeout must be an integer from 1 through 20.
Default: 6 seconds

unregistration *unregistration_timeout*

Configures the timeout value for the unregistration request message sent to the Gatekeeper.
unregistration_timeout must be an integer from 1 through 20.
Default: 3 seconds

Usage

Use this command to configure the timeout interval for the various H.323 requests.

Example

The following command configures the admission request message with a timeout value of *15* seconds:

```
h323 timeout admission 15
```

h323 tpkt

This command allows you to configure the maximum size of Transport Protocol Data Unit Packets (TPKT) that the H.323 Application Layer Gateway (ALG) can handle.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

h323 tpkt *max_tpkt_size*

default h323 tpkt

default

Configures this command with its default setting.
Default: 2048 bytes

max_tpkt_size

Specifies the maximum TPKT size, in bytes.
max_tpkt_size must be an integer from 4 through 4096.

Usage

Use this command to configure the maximum packet size for the H.323 ALG.

Example

The following command configures a maximum TPKT packet size of *100* bytes:

```
h323 tpkt 100
```

h323 version

This command allows you to configure the H.323 version number supported by an H.323 Application Layer Gateway (ALG).

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

h323 version *h323_version_number*

default h323 version

default

Configures this command with its default setting.
Default: 5

h323_version_number

Specifies the H.323 version number.
h323_version_number must be an integer from 1 through 7.

Usage

Use this command to configure the H.323 version number supported by the H.323 ALG.

Example

The following command configures the H.323 version as *1*:

```
h323 version 1
```

host-pool

This command allows you to create/configure/delete host pools.

Product

All

Privilege

Security Administrator, Administrator

Syntax

host-pool *host_pool_name* **[-noconfirm]**

no host-pool *host_pool_name*

no

If previously configured, deletes the specified host pool from the active charging service.

host_pool_name

Specifies the host pool to add/configure/delete.
host_pool_name must be the name of a host pool, and must be a string of 1 through 63 characters, and can contain punctuation characters.
If the named host pool does not exist, it is created, and the CLI mode changes to the ACS Host Pool Configuration Mode wherein the host pool can be configured.
If the named host pool already exists, the CLI mode changes to the ACS Host Pool Configuration Mode for that host pool.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete ACS host pools.
A host pool is a collection of hosts and IP addresses to use in access policy creation. The host pool name must be unique with in the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names. A maximum of the 256 host pools can be created.

Important: Host pools configured in other ruledefs cannot be deleted.

Also see the *ACS Host Pool Configuration Mode Commands* chapter.

Example

The following command creates a host pool named *hostpool1*, and enters the ACS Host Pool Configuration Mode:

```
host-pool hostpool1
```

idle-timeout

This command allows you to configure the maximum duration a flow can remain idle for, after which the system automatically terminates the flow.

Product

ACS, NAT, FW

Privilege

Security Administrator, Administrator

Syntax

idle-timeout { alg-media | flow-mapping { tcp | udp } | icmp | tcp | udp } *idle_timeout*

{ default | no } idle-timeout { alg-media | flow-mapping { tcp | udp } | icmp | tcp | udp }

default

Configures this command with the default setting for the specified parameter.
Default:

- **alg-media**: 120 seconds
- **flow-mapping { tcp | udp }**: 300 seconds for TCP and 0 seconds for UDP
- **icmp**, **tcp**, **udp**: 300 seconds

no

Disables the idle-timeout configuration for the specified flow.

alg-media

Configures the ALG media for the specified flow.

flow-mapping { tcp | udp }

The Flow Mapping timer is an extension to the existing flow idle-timeout in ACS. This flow mapping timeout applies only for NAT enabled calls and is supported only for TCP and UDP flows. The purpose of this timer is to hold the resources (NAT IP, NAT port, Private IP NPU flow) associated with a 5-tuple flow until Mapping timeout expiry.
If the Flow Mapping timer is disabled, then the Mapping timeout will not get triggered for UDP/TCP idle timed out flows. The resources such as NAT mapping will be released along with the 5-tuple flow.

icmp

Configures the ICMP protocol for the specified flow.

tcp

Configures the TCP protocol for the specified flow.

udp

Configures the UDP protocol for the specified flow.

idle_timeout

Specifies the timeout duration, in seconds, and must be an integer from 0 through 86400.
For **alg-media** specifies the media inactivity timeout. The *idle_timeout* value gets applied on RTP and RTCP media flows that are created for SIP/H.323 calls. The timeout is applied only on those flows that actually match the RTP and RTCP media pinholes that are created by the SIP/H.323 ALG.
A value of 0 disables the idle-timeout setting.

Usage

Use this command to configure the maximum duration a flow can remain idle, in seconds, after which the system automatically terminates the flow.
Setting the value to 0 will cause the idle-timeout setting to be disabled.
For flows other than TCP, UDP and ICMP, timeout value will always be 300 seconds (unless configured in the charging-action). Charging action's flow idle-timeout will have precedence over ACS idle-timeout. If charging action's flow idle-timeout is default, then flows will have the value configured in the active charging service.

Example

The following command configures the maximum duration a TCP flow can remain idle to *3000* seconds, after which the system automatically terminates the flow:

```
idle-timeout tcp 3000
```

imsi-pool

This command allows you to create/configure/delete International Mobile Subscriber Identity (IMSI) pools.

Product

All

Privilege

Security Administrator, Administrator

Syntax

imsi-pool *imsi_pool_name* **[-noconfirm]**

no imsi-pool *imsi_pool_name*

no

If previously configured, deletes the specified IMSI pool from the active charging service.

imsi_pool_name

Specifies the IMSI pool to add/configure/delete.
imsi_pool_name must be the name of an IMSI pool, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters.
If the named IMSI pool does not exist, it is created, and the CLI mode changes to the ACS IMSI Pool Configuration Mode wherein the IMSI pool can be configured.
If the named IMSI pool already exists, the CLI mode changes to the ACS IMSI Pool Configuration Mode for that IMSI pool.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete pools of International Mobile Subscriber Identifier (IMSI) numbers having group of single or range of IMSI numbers to use in access policy creation. The IMSI pool name must be unique with in the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names. A maximum of 256 IMSI pools can be created.

Important: IMSI pools configured in other ruledefs cannot be deleted.

Also see the *ACS IMSI Pool Configuration Mode Commands* chapter.

Example

The following command creates an IMSI pool named *imsipool1*, and enters the ACS IMSI Pool Configuration Mode:

```
imsi-pool imsipool1
```

ip dns-learnt-entries

This command allows you to configure how long to keep the snooped IPv4 addresses that were extracted from DNS responses.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip dns-learnt-entries timeout *timeout_period*

{ default | no } ip dns-learnt-entries timeout

default

Configures this command with the default DNS-learnt-entries timeout setting.
Default: 300 seconds

no

Specifies to always use the TTL value in the DNS response, and not the timeout configured with this command.

timeout_period

Specifies the DNS-learnt-entries timeout period, in seconds.
timeout_period must be an integer from 1 through 2147483647.

Usage

Use this command to configure how long to keep the snooped IPv4 addresses that were extracted from DNS responses—for the TTL specified in the DNS response, or for the time period configured with this command, if greater.
The configurable timer will be at global ECS level and shared across all IP addresses. Internally, a five-minute (300 seconds, non configurable) timer will be started whenever DNS analyzer is enabled. On timeout of this timer, all the learnt IP addresses will be checked for TTL expiry and the expired entries will be flushed.

Example

The following command specifies to keep the snooped IPv4 addresses that were extracted from DNS responses for a time period of *900* seconds, or for the TTL value specified in the DNS response, whichever is greater:

```
ip dns-learnt-entries timeout 900
```

ip max-fragments

This command allows you to limit the maximum number of IPv4/IPv6 fragments per fragment chain.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip max-fragments *max_fragments*

default ip max-fragments

default

Configures this command with its default setting.
Default: 45

max_fragments

Specifies the maximum number of IPv4/IPv6 fragments per fragment chain.
max_fragments must be an integer from 1 through 300.

Usage

Use this command to limit the maximum number of IPv4/IPv6 fragments.

Example

The following command limits the maximum number of IPv4/IPv6 fragments to *100*:

```
ip max-fragments 100
```

label content-id

This command allows you to specify a label (text string) to associate with a content ID for UDRs/EDRs/eG-CDRs.

Product

All

Privilege

Security Administrator, Administrator

Syntax

label content-id *content_id* **text** *label_text*

no label content-id *content_id*

no

If previously configured, deletes the specified label.

content-id *content_id*

Specifies the content ID to associate with the label.
content_id must be an integer from 1 through 65535.

text *label_text*

Specifies the label to associate with the specified content ID.
label_text must be an alphanumeric string of 1 through 64 characters.

Usage

Use this command to create a text label to associate with a content ID.
A maximum of 2048 labels can be configured in the active charging service.

Example

The following command creates the label *test_charge1* to be associated with the content ID *1378*:

```
label content-id 1378 text test_charge1
```

nat allocation-failure

This command allows you to configure the action to take when NAT IP/Port allocation fails.

Important: This command is available only in StarOS 8.3 and later releases.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

```
nat allocation-failure send-icmp-dest-unreachable

{ default | no } nat allocation-failure
```

default

Configures this command with its default setting.
Default: Packets are dropped silently

no

If previously enabled, disables the NAT Allocation Failure configuration. Packets are dropped silently.

nat allocation-failure send-icmp-dest-unreachable

Specifies to send ICMP Destination Unreachable message when NAT IP/Port allocation fails.

Usage

Use this command to configure the action to take when NAT IP/port allocation fails—to send or not to send an “ICMP destination unreachable message” when a NAT IP/port cannot be assigned to a flow in data path.

Example

The following command configures sending ICMP Destination Unreachable message when NAT IP/Port allocation fails:

```
nat allocation-failure send-icmp-dest-unreachable
```

nat allocation-in-progress

This command allows you to configure the action to take on packets when NAT IP/NPU allocation is in progress.

Important: This command is available only in StarOS 8.3 and later releases.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

```
nat allocation-in-progress { buffer | drop }

default nat allocation-in-progress
```

default

Configures this command with its default setting.
Default: **buffer**

buffer | drop

Specifies the action to take on packets when NAT IP/NPU allocation is in progress:

- **buffer**: Buffers the packets.
- **drop**:Drops the packets.

Usage

In On-demand NAT IP allocation (wherein NAT IP address is allocated to the subscriber when a packet is being sent), if no free NAT IP address is available, a NAT-IP Alloc Request is sent to the VPNMgr to get NAT-IP. During that time packets are dropped. This command enables buffering the packets received when IP Alloc Request is sent to VPNMgr.

Example

The following command specifies to buffer packets when NAT IP/NPU allocation is in progress:

```
nat allocation-in-progress buffer
```

nat tcp-2msl-timeout

This command allows you to configure the TCP 2MSL (Maximum Segment Lifetime) timeout value for NAT.

Important: This command is available only in StarOS 8.3 and later releases.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

nat tcp-2msl-timeout *timeout*

default nat tcp-2msl-timeout

default

Configures this command with its default setting.
Default: 60 seconds

timeout

Specifies the TCP 2MSL timeout period, in seconds.
timeout must be an integer from 30 through 240.

Usage

Use this command to configure the TCP 2MSL timeout value for NAT.

Example

The following command configures the TCP 2MSL timeout for NAT to *120* seconds:

```
nat tcp-2msl-timeout 120
```

p2p-detection protocol

This command enables/disables the detection of all or specified peer-to-peer (P2P) protocols.

Product

ADC

Privilege

Security Administrator, Administrator

Syntax

[no] p2p-detection protocol [actsync | aimini | all | antsp2p | applejuice | ares | armagettron | battlefld | bittorrent | blackberry | citrix | clubpenguin | crossfire | ddlink | directconnect | dofus | edonkey | facebook | facetime | fasttrack | feidian | fiesta | filetopia | florensia | freenet | fring | funshion | gadugadu | gamekit | gmail | gnutella | gtalk | guildwars | halflife2 | hamachivpn | iax | icecast | imesh | imo | iptv | irc | isakmp | iskoot | itunes | jabber | kontiki | manolito | maplestory | meebo | mgcp | msn | mute | mypeople | myspace | netmotion | nimbuzz | octoshape | off | ogg | oovoo | openft | openvpn | orb | oscar | paltalk | pando | pandora | popo | pplive | ppstream | ps3 | qq | qqgame | qqlive | quake | quicktime | rdp | rdt | rfactor | rmstream | scydo | secondlife | shoutcast | skinny | skype | slingbox | sopcast | soulseek | splashfighter | spotify | ssdp | stealthnet | steam | stun | tango | teamspeak | teamviewer | thunder | tor | truphone | tunnelvoice | tvants | tvuplayer | twitter | ultrabac | usenet | uusee | veohtv | viber | vpnx | vtun | warcft3 | whatsapp | wii | winmx | winny | wmstream | wofkungfu | wofwarcraft | xbox | xdcc | yahoo | yourfreetunnel | zattoo +]

all

Specifies to detect all supported P2P protocols. Specifying **all** is the same as individually configuring each of the following protocols.

actsync

Specifies to detect ActiveSync protocol.

aimini

Specifies to detect Aimini protocol.

antsp2p

Specifies to detect ANts P2P protocol.

applejuice

Specifies to detect Applejuice protocol.

ares

Specifies to detect Ares Galaxy protocol.

armagettron

Specifies to detect Armagetron protocol.

battlefld

Specifies to detect Battlefield protocol.

bittorrent

Specifies to detect BitTorrent protocol.

blackberry

Specifies to detect BlackBerry protocol.

citrix

Specifies to detect Citrix Independent Computing Architecture (ICA) protocol.

clubpenguin

Specifies to detect Club Penguin protocol.

crossfire

Specifies to detect Crossfire protocol.

ddlink

Specifies to detect DDLink protocol.

directconnect

Specifies to detect Direct Connect protocol.

dofus

Specifies to detect DOFUS protocol.

edonkey

Specifies to detect eDonkey protocol.

facebook

Specifies to detect Facebook protocol.

facetime

Specifies to detect FaceTime protocol.

Important: The **facetime** protocol option is available only in 9.0 and in 11.0 and later releases.

fasttrack

Specifies to detect FastTrack protocol.

feidian

Specifies to detect Feidian protocol.

fiesta

Specifies to detect FIESTA protocol.

filetopia

Specifies to detect Filetopia protocol.

florensia

Specifies to detect Florensia protocol.

freenet

Specifies to detect Freenet protocol.

fring

Specifies to detect Fring SIP protocol.

funshion

Specifies to detect Funshion protocol.

gadugadu

Specifies to detect Gadu-Gadu protocol.

gamekit

Specifies to detect GameKit protocol.

Important: The **gamekit** protocol option is available only in 9.0 and in 11.0 and later releases.

gmail

Specifies to detect Gmail protocol.

gnutella

Specifies to detect Gnutella protocol.

gtalk

Specifies to detect Google Talk protocol.

guildwars

Specifies to detect GuildWars protocol.

halflife2

Specifies to detect Half-Life 2 protocol.

hamachivpn

Specifies to detect Hamachi VPN protocol.

iax

Specifies to detect Inter-Asterisk eXchange protocol.

icecast

Specifies to detect Icecast protocol.

imesh

Specifies to detect iMesh protocol.

imo

Specifies to detect Imo.im instant messenger protocol.

iptv

Specifies to detect IPTV protocol.

irc

Specifies to detect Internet Relay Chat protocol.

isakmp

Specifies to detect Internet Security Association and Key Management Protocol.

iskoot

Specifies to detect iSkoot VoIP protocol.

itunes

Specifies to detect iTunes protocol.

jabber

Specifies to detect Jabber XMPP protocol.

kontiki

Specifies to detect Kontiki delivery protocol.

manolito

Specifies to detect MANOLITO protocol.

maplestory

Specifies to detect MapleStory protocol.

meebo

Specifies to detect Meebo protocol.

mgcp

Specifies to detect Media Gateway Control Protocol.

msn

Specifies to detect MSN Messenger protocol.

mute

Specifies to detect MUTE protocol.

mypeople

Specifies to detect My People protocol.

myspace

Specifies to detect MySpace protocol.

netmotion

Specifies to detect NetMotion Internet Mobility Protocol.

nimbuzz

Specifies to detect Nimbuzz protocol.

octoshape

Specifies to detect Octoshape protocol.

off

Specifies to detect Off-The-Record protocol.

ogg

Specifies to detect Ogg multimedia streaming protocol.

oovoo

Specifies to detect ooVoo protocol.

openft

Specifies to detect OpenFT protocol.

openvpn

Specifies to detect OpenVPN protocol.

orb

Specifies to detect Internet Inter-ORB Protocol.

oscar

Specifies to detect Open System for CommunicAtion in Realtime protocol.

paltalk

Specifies to detect Paltalk protocol.

pando

Specifies to detect Pando protocol.

pandora

Specifies to detect Pandora protocol.

popo

Specifies to detect Popo protocol.

pplive

Specifies to detect PPlive protocol.

ppstream

Specifies to detect PPstream protocol.

ps3

Specifies to detect PS3 protocol.

qq

Specifies to detect Tencent QQ instant messaging protocol.

qqgame

Specifies to detect QQgame protocol.

qqlive

Specifies to detect QQlive protocol.

quake

Specifies to detect Quake network protocol.

quicktime

Specifies to detect QuickTime protocol.

rdp

Specifies to detect Remote Desktop protocol.

rdt

Specifies to detect Real Data Transport (RDT) protocol.

rfactor

Specifies to detect rFactor protocol.

rmstream

Specifies to detect RealMedia streaming protocol.

scydo

Specifies to detect Scydo VoIP protocol.

secondlife

Specifies to detect Second Life protocol.

shoutcast

Specifies to detect SHOUTcast protocol.

skinny

Specifies to detect Skinny Call Control Protocol (SCCP).

skype

Specifies to detect Skype protocol.

slingbox

Specifies to detect Slingbox protocol.

sopcast

Specifies to detect Sopcast streaming protocol.

soulseek

Specifies to detect Soulseek chat and file transfer protocol.

splashfighter

Specifies to detect SplashFighter protocol.

spotify

Specifies to detect Spotify music streaming protocol.

ssdp

Specifies to detect Simple Service Discovery Protocol.

stealthnet

Specifies to detect StealthNet RShare network protocol.

steam

Specifies to detect Steam file transfer protocol.

stun

Specifies to detect Session Traversal Utilities for NAT protocol.

tango

Specifies to detect TAco Next Generation Objects hardware control system protocol.

teamspeak

Specifies to detect TeamSpeak VoIP gaming client protocol.

teamviewer

Specifies to detect TeamViewer remote control protocol.

thunder

Specifies to detect Thunder (Xunlei) download manager protocol.

tor

Specifies to detect Tor hidden service (anonymizer) protocol.

truphone

Specifies to detect Truphone WiFi VoIP protocol.

tunnelvoice

Specifies to detect Tunnel VoIP protocol.

tvants

Specifies to detect TVAnts protocol.

tvuplayer

Specifies to detect TVUPlayer protocol.

twitter

Specifies to detect Twitter protocol.

ultrabac

Specifies to detect UltraBac protocol.

usenet

Specifies to detect Usenet Network News Transfer Protocol (NNTP) protocol.

uusee

Specifies to detect UUSee on-demand streaming protocol.

veohtv

Specifies to detect VeohTV television via Internet protocol.

viber

Specifies to detect Viber VoIP protocol.

vpnx

Specifies to detect VPN-X cross-platform protocol.

vtun

Specifies to detect VTun (Virtual Tunnel) protocol.

warcft3

Specifies to detect Warcraft 3 game protocol.

whatsapp

Specifies to detect WhatsApp messaging protocol.

wii

Specifies to detect Wii Remote Bluetooth protocol.

winmx

Specifies to detect WinMX Peer Network Protocol (WPNP).

winny

Specifies to detect Winny anonymizing protocol.

wmstream

Specifies to detect Windows Media HTTP Streaming Protocol.

wofkungfu

Specifies to detect wofkungfu protocol.

wofwarcraft

Specifies to detect World of Warcraft gaming protocol.

xbox

Specifies to detect Xbox protocol.

xdcc

Specifies to detect eXtended Direct Client-to-Client protocol.

yahoo

Specifies to detect Yahoo! Messenger protocol.

yourfreetunnel

Specifies to detect your free Tunnel chat protocol.

zattoo

Specifies to detect Zattoo IPTV protocol.

+

More than one of the above keywords can be entered within a single command.

Usage

Use this command to configure the detection of all or specific P2P protocol(s). Multiple keywords can be specified in a single command.

Example

The following command enables detection of all P2P protocols:

```
p2p-detection protocol all
```

packet-filter

This command allows you to create/configure/delete ACS packet filters.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

packet-filter *packet_filter_name* **[-noconfirm]**

no packet-filter *packet_filter_name*

no

If previously configured, deletes the specified packet filter from the active charging service.

packet_filter_name

Specifies the packet filter to add/configure/delete.
packet_filter_name must be the name of a packet filter, and must be an alphanumeric string of 1 through 63 characters.
If the named packet filter does not exist, it is created, and the CLI mode changes to the ACS Packet Filter Configuration Mode wherein the packet filter can be configured.
If the named packet filter already exists, the CLI mode changes to the ACS Packet Filter Configuration Mode for that packet filter.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete an ACS packet filter.
Also see the *ACS Packet Filter Configuration Mode Commands* chapter.

Example

The following command creates a packet filter named *filter3*, and enters the ACS Packet Filter Configuration Mode:

```
packet-filter filter3
```

passive-mode

This command allows you to configure the Active Charging Service to operate in passive mode, wherein ACS passively monitors copies of packets.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] passive-mode
```

no

If previously enabled, disables the passive mode configuration.

default

Configures this command with its default setting.
Default: Disabled

Usage

Use this command to put the active charging service in/out of passive mode operation, wherein ACS passively monitors copies of packets.

Example

The following command puts the active charging service into passive mode operation:

```
passive-mode
```

policy-control bearer-bw-limit

This command allows you to enable/disable per-bearer MBR policing—bandwidth limiting.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
{ default | no } policy-control bearer-bw-limit
```

default

Configures this command with its default setting.
Default: Enable; by default, per-bearer MBR policing is enabled.

no

Disables per-bearer MBR policing.

Usage

This command allows you to enable/disable per-bearer bandwidth limiting based on bitrates received over Gx. Note that there are only two variants of this command, the default and no variants.

policy-control bind-default-bearer

For PCEF Bearer Binding in 3G and when BCM mode is UE only, this command allows you to enable/disable binding rules having QCI of default bearer to the default bearer and to not ignore/ignore other rules.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] policy-control bind-default-bearer
```

default

Configures this command with its default setting.
Default: Disables binding rules having QCI of default bearer to the default bearer and specifies to not ignore other rules.

no

Enables binding rules having QCI of default bearer to the default bearer and specifies to ignore other rules.

Usage

For PCEF Bearer Binding in 3G and when BCM mode is UE only, use this command to enable/disable binding rules having QCI of default bearer to the default bearer and to not ignore/ignore other rules respectively.

policy-control burst-size

This command allows you to configure the burst size for bandwidth limiting per dynamic-rule or per bearer.

Product

All

Privilege

Security Administrator, Administrator

Syntax

policy-control burst-size { auto-readjust [duration *duration* **] | bytes** *bytes* **}**

{ default | no } policy-control burst-size

default | no

Configures this command with its default setting.
Default: 65535 bytes

duration *duration*

Configures the burst size equal to <seconds> of traffic.
duration must be an integer from 1 through 20.
Default: In 12.1 and earlier releases, 10 seconds. In 12.2 and later releases, 5 seconds.

bytes *bytes*

Specifies the burst size, in bytes.
bytes must be an integer from 1 through 4000000000.

Usage

Use this command to configure the burst size for bandwidth limiting per dynamic-rule or per bearer.

Example

The following command configures the burst size for bandwidth limiting per dynamic-rule or per bearer equal to 10 seconds of traffic:

```
policy-control burst-size auto-readjust
```

policy-control charging-action-override

This command allows you to enable/disable overriding charging parameters of static rule with those of an ip-any rule or a specified dynamic rule.

Important: This command is customer specific. For more information contact your Cisco account representative.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

policy-control charging-action-override custom1 [use-rule *dynamic_rule_name* **]**

{ default | no } policy-control charging-action-override

default

Configures this command with its default setting.
Default: Enables overriding charging parameters of static rule with those of an ip-any or a specified dynamic rule.

no

Disables overriding charging parameters of static rule with those of an ip-any or a specified dynamic rule.

custom1

Specifies overriding Online/Offline, Service ID, Content ID, Flow Control, ARP, and QCI.

use-rule *dynamic_rule_name*

Optional: Specifies the dynamic rule to inherit charging parameters from. If a dynamic rule name is not specified, the charging properties will be inherited from any dynamic rule.
dynamic_rule_name specifies name of the dynamic rule, and must be an alpha and/or numeric string of 1 through 63 characters in length.

Usage

Use this command to enable/disable overriding charging parameters of static rule with those of a dynamic ip-any rule or a specified dynamic rule.

Example

The following command specifies to enable overriding charging parameters of static rule with those of a dynamic rule named *test*:

```
policy-control charging-action-override custom1 use-rule test
```

policy-control charging-rule-base-name

This command allows you to configure how the Charging-Rule-Base-Name AVP from PCRF is interpreted, either as ACS rulebase or ACS group-of-ruledefs.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
policy-control charging-rule-base-name { active-charging-group-of-ruledefs | active-charging-rulebase [ ignore-when-removed ] [ use-first ]}

default policy-control charging-rule-base-name

no policy-control charging-rule-base-name active-charging-rulebase use-first
```

default

Configures this command with its default setting(s).
Default:

- **charging-rule-base-name**: **active-charging-group-of-ruledefs**
- **use-first**: Disabled

no

If multiple Charging-Rule-Base-Name are received from the PCRF, specifies to select the last rulebase. This is the default behavior.

active-charging-group-of-ruledefs

Specifies interpreting Charging-Rule-Base-Name as ACS group-of-ruledefs.

active-charging-rulebase [ignore-when-removed][use-first]

Specifies interpreting Charging-Rule-Base-Name as ACS rulebase.
When Charging-Rule-Base-Name AVP is interpreted as ACS rulebase, if PCRF requests the removal of a Charging-Rule-Base-Name, which is the same as the rulebase used for that PDP context, the PDP context is terminated. This is because after removal of the rulebase, the PDP context will have no rulebase. This is the default behavior.
ignore-when-removed: Specifies to ignore PCRF request for removal of Charging-Rule-Base-Name, and take no action. If this keyword is not configured, the PDP context from which the rulebase is removed gets terminated.
use-first: If multiple Charging-Rule-Base-Name are received from the PCRF, since a call can only have one ACS rulebase applied, specifies to select the first rulebase. If previously enabled, to disable this configuration, use the **no policy-control charging-rule-base-name active-charging-rulebase use-first** command. If this keyword is not configured, by default, the last rulebase is selected. For each call, this interpretation is decided at call setup, and will not be changed during the life of that call. Change will only apply to new calls coming up after the change.

Usage

Use this command to configure interpretation of Charging-Rule-Base-Name AVP from PCRF either as ACS group-of-ruledefs or as ACS rulebase.

Example

The following command configures interpreting of Charging-Rule-Base-Name AVP as ACS rulebase:

```
policy-control charging-rule-base-name active-charging-rulebase
```

policy-control dynamic-rule-limit

This command allows you to enable/disable per-dynamic-rule MBR policing—bandwidth limiting.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
{ default | no } policy-control dynamic-rule-limit
```

default

Configures this command with its default setting.
Default: Enable; by default, per-dynamic-rule MBR policing is enabled.

no

Disables per-dynamic-rule MBR policing.

Usage

This command allows you to enable/disable per-dynamic-rule bandwidth limiting based on bitrates received over Gx. Note that there are only two variants of this command, the default and no variants.

policy-control retransmissions-counted

This command allows you to enable/disable charging of retransmitted packets when they hit a dynamic rule.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] policy-control retransmissions-counted
```

default | no

Disables charging of retransmitted packets when they hit a dynamic rule.
Default: Disabled; no retransmissions counted.

Usage

Use this command to enable/disable charging of retransmitted packets when they hit a dynamic rule.

Example

The following command enables retransmissions to be charged when they hit a dynamic rule:

```
policy-control retransmissions-counted
```

policy-control update-default-bearer

For PCEF Bearer Binding in LTE, this command allows you to enable/disable sending updates that control the default bearer to the subscriber.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] policy-control update-default-bearer
```

default

Configures this command with its default setting.
Default: Enables sending updates towards subscriber on default bearer.

no

Disables sending updates towards subscriber on default bearer.

Usage

For PCEF Bearer Binding in LTE, use this command to enable/disable sending updates like change in TFT, change in bit-rates, and so on towards the subscriber, in downlink direction, on default bearer.

port-map

This command allows you to create/configure/delete port maps.

Product

All

Privilege

Security Administrator, Administrator

Syntax

port-map *port_map_name* **[-noconfirm]**

no port-map *port_map_name*

no

If previously configured, deletes the specified port map from the active charging service.

port_map_name

Specifies the port map to add/configure/delete.
port_map_name must be the name of a port map, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters.
If the named port map does not exist, it is created, and the CLI mode changes to the ACS Port Map Configuration Mode wherein the port map can be configured.
If the named port map already exists, the CLI mode changes to the ACS Port Map Configuration Mode for that port map.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete an ACS port map.
The port map name must be unique with in the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names. A maximum of the 256 port maps can be created.

Important: Port maps in use in other ruledefs cannot be deleted.

Also see the *ACS Port Map Configuration Mode Commands* chapter.

Example

The following command creates a port map named *portmap1*, and enters the ACS Port Map Configuration Mode:

```
port-map portmap1
```

redirect user-agent

This command allows you to specify the user agent for conditional redirection of traffic flows.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] redirect user-agent *user_agent_name*

no

If previously configured, deletes the specified user agent from the active charging service.

user_agent_name

Specifies the user agent to be used for redirecting traffic flow.
user_agent_name must be the name of a user agent, and must be an alphanumeric string of 1 through 32 characters.
A maximum of 16 user-agents can be configured in the active charging service.

Usage

Use this command to redirect the traffic flow with conditions based on configured user-agent name. This user agent is used with **flow action** command in the ACS Charging Action Configuration Mode.

Example

The following command specifies the redirect user agent *user_rule1* for conditional redirection of traffic flow:

```
redirect user-agent user_rule1
```

rulebase

This command allows you to create/configure/delete ACS rulebases.

Important: A maximum of 512 rulebases can be configured in the active charging service.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
rulebase rulebase_name [ -noconfirm ]

no rulebase rulebase_name
```

no

If previously configured, deletes the specified rulebase from the active charging service.

rulebase_name

Specifies the rulebase to add/configure/delete.
rulebase_name must be the name of an ACS rulebase, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters.
If the named rulebase does not exist, it is created, and the CLI mode changes to the ACS Rulebase Configuration Mode wherein the rulebase can be configured.
If the named rulebase already exists, the CLI mode changes to the ACS Rulebase Configuration Mode for that rulebase.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete an ACS rulebase. A rulebase is a collection of protocol rules to match a flow and associated actions to be taken for matching flow. The *rulebase_name* must be unique in the active charging service.
The default rulebase is used when a subscriber/APN is not configured with a specific rulebase to use.
Also see the *ACS Rulebase Configuration Mode Commands* chapter.

Example

The following command creates a rulebase named *test1*, and enters the ACS Rulebase Configuration Mode:

```
rulebase test1
```

ruledef

This command allows you to create/configure/delete ACS rule definitions.

Important: A maximum of 2048 ruledefs can be configured in the active charging service.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

ruledef *ruledef_name* **[-noconfirm]**

no ruledef *ruledef_name*

no

If previously configured, deletes the specified ruledef from the active charging service.

ruledef_name

Specifies the ruledef to add/configure/delete.
ruledef_name must be the name of an ACS ruledef, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters.
ruledef_name must be unique with in the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names.
If the named ruledef does not exist, it is created, and the CLI mode changes to the ACS Ruledef Configuration Mode wherein the ruledef can be configured.
If the named ruledef already exists, the CLI mode changes to the ACS Ruledef Configuration Mode for that ruledef.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete an ACS ruledef.
A ruledef represents a set of matching conditions across multiple L3 – L7 protocol based on protocol fields and state information. Each ruledef can be used across multiple rulebases within the active charging service.
Also see the *ACS Ruledef Configuration Mode Commands* chapter.

Example

The following command creates an ACS ruledef named *test1*, and enters the ACS Ruledef Configuration Mode:

```
ruledef test1
```

system-limit l4-flows

This command allows you to configure the system-wide Layer 4 flow limit.

Important: This command is customer specific. For more information contact your Cisco account representative.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

system-limit l4-flows *limit*

{ default | no } system-limit l4-flows

default

Configures this command with its default setting.
Default: Disabled; same as **no system-limit l4-flows**

no

Disables the limit checking configuration.

limit

Specifies the Layer 4 flows limit.
limit must be an integer from 1 through 2147483647.

Usage

Use this command to configure the system-wide limit for Layer 4 flows.
The System-wide L4 Flow Limiting feature provides the capability to limit the number of TCP and UDP flow over the system. This limiting can be applied to all subscribers attaching to the system and to all APNs. This feature is compatible with the existing per-subscriber limiting (configured using the flow limit-for-flow-type charging action). Both limiting can be active in the same time.
System-wide flow limiting is implemented by comparing the "Effective Flows" periodically (~ every 10 seconds) against the configurable "System-wide Flow Limit". Where "Effective Flows" is the number of active data sessions, each identified by the 5-tuple key. If the "Effective Flows" exceeds the "System-wide Flow Limit", the Resource Manager indicates it to the active charging service. When ACS is aware of the "System-wide Flow Limit" being reached, no more data sessions are setup. The packets are discarded. While processing a successive flow-usage update from active charging service a change in behavior is indicated to active charging service to start accepting data sessions. As this relies on periodic reporting there is an inherent delay in the detection of "exceeding/returning once exceeded" to the flow limit.

Example

The following command sets the system limit for L4 flows to *100*:

```
system-limit l4-flows 100
```

tethering-database

This command allows you to enable/disable the Tethering Detection feature, and load the databases from the specified files into the service.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

tethering-database [os-signature *os_signature_db_file_name* **| tac** *tac_db_file_name* **| ua-signature** *ua_signature_db_file_name* **] +**

{ default | no } tethering-database

default

Configures this command with its default setting.
Default: Tethering Detection feature is disabled, and the database file names are reset to their default values.

no

Disables Tethering Detection.

tethering-database os-signature *os_signature_db_file_name*

Specifies the OS Signature database file to load.
os_signature_db_file_name must be the name of the OS Signature database file, and must be an alphanumeric string of 1 through 255 characters.

tethering-database tac *tac_db_file_name*

Specifies the TAC database file to load.
tac_db_file_name must be the name of a TAC database file, and must be an alphanumeric string of 1 through 255 characters.

tethering-database ua-signature *ua_signature_db_file_name*

Specifies the User Agent (UA) Signature database file to load.
ua_signature_db_file_name must be the name of a UA Signature database file, and must be an alphanumeric string of 1 through 255 characters.

+

Indicates that more than one of the preceding option can be entered in a single command.

Usage

Use this command to enable the Tethering Detection feature, and load the OS, TAC, and UA databases from the specified files into the service.
Tethering refers to the use of a smartphone as a USB dongle/modem to provide Internet connectivity to laptops/PDAs/tablets like iPad, using the smartphone's data plan. Typically many operators have in place an

eat-all-you-can-get data plan for smartphones, the usage of which is intended to be from the smartphone as a mobile device. However, some users use the low rate/unlimited usage of data plan to provide Internet connectivity to their laptops in places where normal Internet connection via broadband/WiFi might be more costly/not available/insecure.
Operators are interested in detecting such usage of a smartphone as a modem to better understand the usage across their networks and offer plans inline to that usage to their customers. They may also charge the tethered and non-tethered traffic separately.
After Tethering Detection has been enabled here (regardless, it must also be enabled within the rulebase), this CLI command may be used to change the databases with the specified databases.
The files are picked from the disk file system within the /databases directory. If a file name value is not configured, the default file names, *os-db*, *tac-db*, and *ua-db*, are used.
For more information on the Tethering Detection feature, refer to the *Enhanced Charging Services Administration Guide*.

Example

The following command enables Tethering Detection and selects the UA Signature database file named *test*:

```
tethering-database ua-signature test
```

timedef

This command allows you to create/configure/delete ACS Time Definitions (timedefs).

Important: This command is available only in StarOS 8.1 and in StarOS 9.0 and later releases.

Important: A maximum of 10 timedefs can be configured in the active charging service.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

timedef *timedef_name* **[-noconfirm]**

no timedef *timedef_name*

no

If previously configured, deletes the specified timedef from the active charging service.

timedef_name

Specifies the timedef to add/configure/delete.
timedef_name must be the name of a timedef, and must be an alphanumeric string of 1 through 63 characters.
If the named timedef does not exist, it is created, and the CLI mode changes to the ACS Timedef Configuration Mode wherein timeslots for the timedef can be configured.
If the named timedef already exists, the CLI mode changes to the ACS Timedef Configuration Mode for that timedef.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete ACS timedefs for the Time-of-Day Activation/Deactivation of Rules feature. Timedefs enable activation/deactivation of ruledefs/groups-of-ruledefs such that they are available for rule matching only when they are active.
Also see the *ACS Timedef Configuration Mode Commands* chapter.

Example

The following command creates a timedef named *test1*, and enters the ACS Timedef Configuration Mode:

```
timedef test1
```

tpo policy

This command allows you to create/configure/delete Traffic Performance Optimization (TPO) policies.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

tpo policy *tpo_policy_name* **[-noconfirm]**

no tpo policy *tpo_policy_name*

no

If previously configured, deletes the specified TPO policy from the active charging service.

tpo_policy_name

Specifies the TPO policy to add/configure/delete.
tpo_policy_name must be the name of a TPO policy, and must be an alphanumeric string of 1 through 63 characters.
If the named TPO policy does not exist, it is created, and the CLI mode changes to the ACS TPO Policy Configuration Mode wherein the TPO policy can be configured.
If the named TPO policy already exists, the CLI mode changes to the ACS TPO Policy Configuration Mode for that TPO policy.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Important: A maximum of 2048 TPO policies can be created in the active charging service.

Use this command to create/configure/delete TPO policies.
A TPO Policy contains the rules that determine which TPO profile is to be used.
Also see the *ACS TPO Policy Configuration Mode Commands* chapter.

Example

The following command creates a TPO policy named *tpo_policy_1*, and enters the ACS TPO Policy Configuration Mode:

```
tpo policy tpo_policy_1
```

tpo profile

This command allows you to create/configure/delete Traffic Performance Optimization (TPO) profiles.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

tpo profile *tpo_profile_name* **[-noconfirm]**

no tpo profile *tpo_profile_name*

no

If previously configured, deletes the specified TPO profile from the active charging service.

tpo_profile_name

Specifies the TPO profile to add/configure/delete.
tpo_profile_name must be the name of a TPO profile, and must be an alphanumeric string of 1 through 63 characters.
If the named TPO profile does not exist, it is created, and the CLI mode changes to the ACS TPO Profile Configuration Mode wherein the TPO profile can be configured.
If the named TPO profile already exists, the CLI mode changes to the ACS TPO Profile Configuration Mode for that TPO profile.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Important: A maximum of 2048 TPO profiles can be created in the active charging service.

Use this command to create/configure/delete TPO profiles.
A TPO profile contains the optimization configuration to be used.
Also see the *ACS TPO Profile Configuration Mode Commands* chapter.

Example

The following command creates a TPO profile named *tpo_profile_1*, and enters the ACS TPO Profile Configuration Mode:

```
tpo profile tpo_profile_1
```

udr-format

This command allows you to create/configure/delete a User Data Record (UDR) format.

Product

All

Privilege

Security Administrator, Administrator

Syntax

udr-format *udr_format_name* **[-noconfirm]**

no udr-format *udr_format_name*

no

If previously configured, deletes the specified UDR format from the active charging service.

udr_format_name

Specifies the UDR format to add/configure/delete.
udr_format_name must be the name of a UDR format, and must be an alphanumeric string of 1 through 63 characters.
If the named UDR format does not exist, it is created, and the CLI mode changes to the UDR Format Configuration Mode wherein the UDR format can be configured.
If the named UDR format already exists, the CLI mode changes to the UDR Format Configuration Mode for that UDR format.
Up to 256 UDR and/or EDR formats can be configured in the active charging service.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete a UDR format in the active charging service.
Also see the *UDR Format Configuration Mode Commands* chapter.

Example

The following command creates an UDR format named *udr_fromat1* and changes to the UDR Format Configuration Mode:

```
udr-format udr_format1
```

url-blacklisting match-method

This command allows you to specify the match method to look up URLs in the URL Blacklisting database.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

```
url-blacklisting match-method { exact | generic }

default url-blacklisting match-method
```

default

Configures this command with its default setting.
Default: **exact**

exact

Specifies the exact-match method, wherein URL Blacklisting is performed only on exact match with a URL present in the URL Blacklisting database.

generic

Specifies the generic-match method, wherein URL Blacklisting is performed on a generic match with URLs present in the URL Blacklisting database.

Usage

Use this command to set the match method to look up URLs in the URL Blacklisting database.

Example

The following command sets the exact-match method to look up URLs in the URL Blacklisting database:

```
url-blacklisting match-method exact
```

xheader-format

This command allows you to create/configure/delete ACS extension-header (x-header) format specifications.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

xheader-format *xheader_format_name* **[-noconfirm]**

no xheader-format *xheader_format_name*

no

If previously configured, deletes the specified x-header format from the active charging service.

xheader_format_name

Specifies the x-header format to add/configure/delete.
xheader_format_name must be the name of an xheader format, and must be an alphanumeric string of 1 through 63 characters.
If the named x-header format does not exist, it is created, and the CLI mode changes to the ACS X-header Format Configuration Mode wherein the x-header format can be configured.
If the named x-header format already exists, the CLI mode changes to the ACS X-header Format Configuration Mode for that x-header format.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete an x-header format specification in the active charging service.
An x-header may be specified in a charging action to be inserted into HTTP GET and POST request packets.
See **xheader-insert** CLI command in the *ACS Charging Action Configuration Mode Commands* chapter.
Also see the *ACS X-header Format Configuration Mode Commands* chapter.

Example

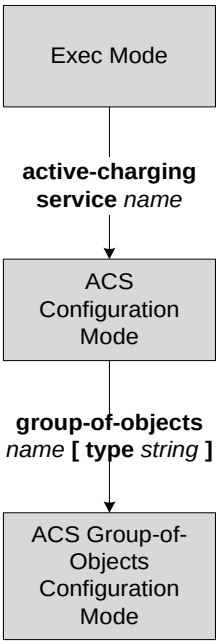
The following command creates an x-header format named *test*, and enters the ACS X-header Format Configuration Mode:

```
xheader-format test
```

Chapter 9
ACS Group-of-Objects Configuration Mode Commands

The ACS Group-of-Objects Configuration Mode is used to configure groups of Active Charging Service (ACS) objects.

Important: This configuration mode is available only in 10.2 and later releases.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

member-object

This command allows you to add or remove objects from the current group-of-objects.

Important: A maximum of 128 objects can be added to a group-of-objects.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] member-object *object*

no

If previously added, removes the specified member object from the current group-of-objects.

object

Specifies the member object to add to or remove from the current group-of-objects.
object must be an alpha and/or numeric string of 1 through 63 characters.

Usage

Use this command to add or remove member objects from a group-of-objects.

Example

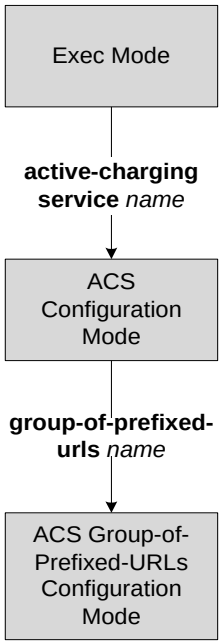
The following command adds the object *test* to the current group-of-objects:

```
member-object test
```

Chapter 10
ACS Group-of-Prefixed-URLs Configuration Mode Commands

The ACS Group-of-Prefixed-URLs Configuration Mode is used to create and configure groups of prefixed URLs.

Important: This configuration mode is customer specific. For more information, contact your Cisco account representative.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

prefixed-url

This command allows you to add or remove URLs from the current group of prefixed URLs.

Important: A maximum of 10 URLs can be added per group.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] prefixed-url` *`url`*

`no`

If added previously, removes the specified URL from the current group of prefixed URLs.

`url`

Specifies the URL to add/remove.
`url` must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to add or remove URLs to be filtered from the group of prefixed URLs.

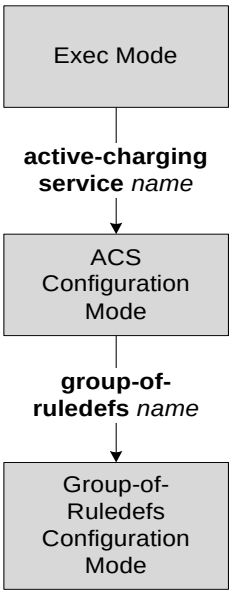
Example

The following command adds the URL *`http://abc.net`* to the current group of prefixed URLs:

```
prefixed-url http://abc.net
```

Chapter 11
ACS Group-of-Ruledefs Configuration Mode Commands

The ACS Group-of-Ruledefs Configuration Mode is used to configure groups of rule definitions (ruledefs).



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

add-ruledef

This command allows you to add or remove ruledefs from a group-of-ruledefs.

Important: A maximum of 128 ruledefs can be added to a group-of-ruledefs.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

add-ruledef priority *ruledef_priority* **ruledef** *ruledef_name*

no add-ruledef priority *ruledef_priority*

no

If previously configured, specifies that the ruledef associated with the specified priority number be removed from the current group-of-ruledefs.

priority *ruledef_priority*

Specifies priority of the ruledef in the current group-of-ruledefs.
ruledef_priority must be unique in the group-of-ruledefs, and must be an integer from 1 through 10000.

ruledef *ruledef_name*

Specifies name of the ruledef to add to the current group-of-ruledefs.
ruledef_name must be the name of an ACS ruledef, and must be an alpha and/or numeric string of 1 through 63 characters.

Usage

Use this command to add/remove ruledefs from a group-of-ruledefs.
A group-of-ruledefs can contain optimizable ruledefs. Whether a group is optimized or not is decided on whether all the ruledefs in the group-of-ruledefs can be optimized, and if the group is included in a rulebase that has optimization turned on, then the group will be optimized.
When a new ruledef is added, it is checked if it is included in any group-of-ruledefs, and whether it needs to be optimized, etc.

Example

The following command adds the ruledef *ruledef23* to the current group-of-ruledefs, and assigns it a priority of *3*:

```
add-ruledef priority 3 ruledef ruledef23
```

dynamic-command

This command allows you to add or remove dynamic commands from a group-of-ruledefs.

Product

ACS, CF

Privilege

Security Administrator, Administrator

Syntax

dynamic-command content-filtering category policy-id *policy_id*

no dynamic-command content-filtering category policy-id

no

Specifies to remove dynamic command configuration from the current group-of-ruledefs.

content-filtering category policy-id *policy_id*

Specifies the dynamic command for Content Filtering Category Policy ID configuration. *policy_id* must be a Content Filtering Category Policy ID, and must be an integer from 1 through 4294967295.

Usage

Use this command to add a dynamic command to a group-of-ruledefs, which will be executed when a dynamic protocol specifies that group-of-ruledefs (via the Rulebase-Name AVP).

Important: This release supports only one command option, which is **dynamic-command content-filtering category policy-id** *policy_id*

Example

The following command configures a dynamic command for Content Filtering Category Policy ID configuration using the policy ID *100*:

```
dynamic-command content-filtering category policy-id 100
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

group-of-ruledefs-application

This command allows you to specify the purpose of setting up a group-of-ruledefs as either charging, post-processing, or for other purposes.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
group-of-ruledefs-application { charging | content-filtering | gx-alias | post-processing
| tpo }

no group-of-ruledefs-application
```

no

If previously configured, deletes the group-of-ruledefs-application configuration from the current group-of-ruledefs.

charging

Specifies that the current group-of-ruledefs is for charging purposes.

content-filtering

Specifies that the current group-of-ruledefs is for content-filtering purposes.

gx-alias

Specifies that the current group-of-ruledefs is for Gx-alias purposes.

post-processing

Specifies that the current group-of-ruledefs is for post-processing purposes, that is, for use by the **post-processing** CLI command or automatic name-matching to the Diameter Filter-Id AVPs.

tpo

Important: The **tpo** keyword is available only in 12.2 and later releases.

Specifies that this group-of-ruledefs is for use in Traffic Performance Optimization (TPO) in-line service's match-rule and match-advertisement configurations.
TPO can use both "charging" and "tpo" rule-application types. Note that ruledef/group-of-ruledef statistics are computed only for the "tpo" rule-application type. In the case of charging ruledefs/group-of-ruledefs, statistics are not computed, and are allowed only for backward compatibility. To generate ruledef statistics use "tpo" ruledefs in the TPO policies.
Default: Disabled

Usage

Use this command to specify the purpose of setting up a group-of-ruledefs. If not specified, by default the rule-application type will be charging.

If the group-of-ruledefs-application is configured for content-filtering, no ruledef can be added to it. Similarly, if configured explicitly for charging or post-processing, a content-filtering policy cannot be configured in it.

The group-of-ruledefs may be dynamically selected by Diameter, as described by the **policy-control charging-rulebase-name** command in the Active Charging Service Configuration Mode. If so selected, the priority field of the add-ruledef instances within the group-of-ruledefs are ignored, and all of the rules named by the ruledef keyword that are also configured with the same name in the **action** command are selected.

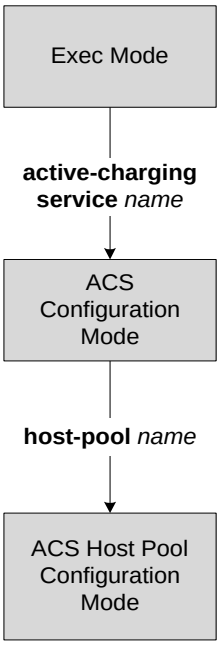
Example

The following command configures the current group-of-ruledefs as for post-processing purposes:

```
group-of-ruledefs-application post-processing
```

Chapter 12
ACS Host Pool Configuration Mode Commands

The ACS Host Pool Configuration Mode is used to define a pool of host addresses within the ACS Configuration Mode. The host pool facilitates to create rules to handle the packets coming from or going to a group of hosts within an access policy.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

ip

This command allows you to add/remove an individual or a range of host IPv4/IPv6 address(es) from the current host pool.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] ip { *ip_address* **|** *ip_address***/***maskbit* **| range** *start_ip* **to** *end_ip* **}**

no

If added previously, removes the specified IPv4/IPv6 address(es) from the current host pool.

ip_address

Specifies an IPv4/IPv6 address to add to the current host pool.
ip_address must be an IPv4/IPv6 address.

*ip_address***/***maskbit*

Specifies an IPv4/IPv6 address/mask bits combination to add to the current host pool.
ip_address must be an IPv4/IPv6 address.
maskbit must be the number of bits in the subnet mask, and must be a numeric value.

range *start_ip* **to** *end_ip*

Specifies a range of IPv4/IPv6 addresses to add to the current host pool.
start_ip specifies the starting IPv4/IPv6 address of the range, and must be less than *end_ip*.
end_ip specifies the ending IPv4/IPv6 address of the range, and must be greater than *start_ip*.

Usage

Use this command to add an individual or a range of IPv4/IPv6 addresses to a host pool. Up to 10 sets of IPv4/IPv6 addresses can be configured in each host pool.

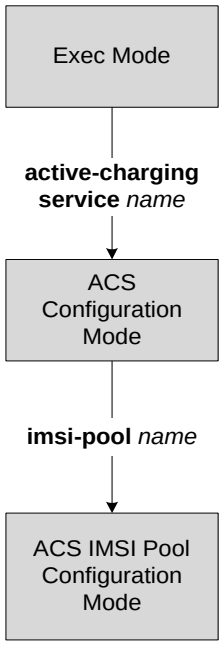
Example

The following command adds all IPv4 addresses from *10.2.3.4* through *10.4.5.6* to the current host pool:

```
ip range 10.2.3.4 to 10.4.5.6
```

Chapter 13
ACS IMSI Pool Configuration Mode Commands

The ACS IMSI Pool Configuration Mode is used to define a pool of subscriber International Mobile Station Identifier (IMSI) numbers within the ACS Configuration Mode. IMSI pool configuration facilitates creation of rules to handle the packets coming from or going to a group of subscriber of IMSI numbers within an access policy.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

imsi

This command allows you to add/remove an individual or a range of subscriber IMSI numbers from the current IMSI pool.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] imsi { *imsi_number* **| range** *start_imsi* **to** *end_imsi* **}**

no

If added previously, removes the specified subscriber IMSI number(s) from the current IMSI pool.

imsi_number

Specifies an IMSI number to add to the current IMSI pool.
imsi_number must be an IMSI number, and must be a sequence of hexadecimal digits between 1 and 15.

start_imsi **to** *end_imsi*

Specifies a range of IMSI numbers to add to the current IMSI pool.
start_imsi specifies the starting IMSI number of the range and must be less than *end_imsi*.
end_imsi specifies the ending IMSI number of the range and must be greater than *start_imsi*.

Usage

Use this command to add an individual or range of subscriber IMSI numbers to an IMSI pool. Up to 10 sets of IMSI numbers can be configured in each IMSI pool.

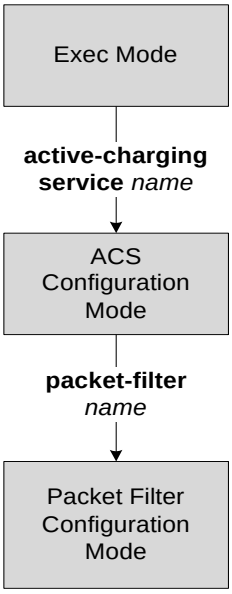
Example

The following command adds IMSI numbers from *310150987654321* to *310150987656879* to the current IMSI pool:

```
imsi range 310150987654321 to 310150987656879
```

Chapter 14
ACS Packet Filter Configuration Mode Commands

The ACS Packet Filter Configuration Mode is used to create and configure Active Charging Service (ACS) packet filters.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

direction

This command allows you to specify the direction in which the current packet filter will be applied.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
direction { bi-directional | downlink | uplink }

default direction
```

default

Configures this command with its default setting.
Default: **bi-directional**

bi-directional

Specifies that the packet filter has to be applied in both uplink and downlink directions.

downlink

Specifies that the packet filter has to be applied only in the downlink direction.

uplink

Specifies that the packet filter has to be applied only in the uplink direction.

Usage

Use this command to specify the direction in which the packet filter has to be applied.

Example

The following command specifies that the packet filter must be applied in the downlink direction:

```
direction downlink
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

ip local-port

This command allows you to configure the IP 5-tuple local port(s) for the current packet filter.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

ip local-port { = *port_number* | range *start_port_number* to *end_port_number* }

no ip local-port

no

If previously configured, deletes the ip local-port configuration from the current packet filter.

port_number

Specifies the port number of the transport protocol.
port_number must be the port number, and must be an integer from 1 through 65535.

range *start_port_number* **to** *end_port_number*

Specifies a range of port numbers.
start_port_number and *end_port_number* must be integers from 1 through 65535.
end_port_number must be greater than *start_port_number*.

Usage

Use this command to configure the IP local port(s) for a packet filter.

Example

The following command configures the IP local port as *456*:

```
ip local-port 456
```

ip protocol

This command allows you to configure the IP protocol(s) for the current packet filter.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

In StarOS 8.x releases:

ip protocol { = *protocol_number* **| range** *start_protocol_number* **to** *end_protocol_number* **}**

no ip protocol

In StarOS 9.0 and later releases:

ip protocol = *protocol_number*

no ip protocol

no

If previously configured, deletes the IP protocol configuration from the current packet filter.

protocol_number

Specifies the transport protocol field in the IP header.
protocol_number must be the numerical value of the protocol, and must be an integer from 1 through 255.

range *start_protocol_number* **to** *end_protocol_number*

Important: In StarOS 9.0 and later releases this option is deprecated.

Specifies a range of protocol assignment numbers.
start_protocol_number and *end_protocol_number* must be integers from 1 through 255.
end_protocol_number must be greater than *start_protocol_number*.

Usage

Use this command to configure the protocol(s) for a packet filter.

Example

The following command configures the protocol assignment number *300*:

```
ip protocol = 300
```

ip remote-address

This command allows you to configure the IP remote address(es) for the current packet filter.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

In StarOS 8.x releases:

ip remote-address { = { *ip_address* | *ip_address/mask* } | range { *ip_address* | *ip_address/mask* } to { *ip_address* | *ip_address/mask* } }

no ip remote-address

In StarOS 9.0 and later releases:

ip remote-address = { *ip_address* | *ip_address/mask* }

no ip remote-address

no

If previously configured, deletes the IP remote-address configuration from the current packet filter.

ip remote-address = { *ip_address* | *ip_address/mask* }

ip_address specifies the IPv4/IPv6 address.
ip_address/mask specifies the IPv4/IPv6 address and the number of subnet bits representing the subnet mask in shorthand.

ip remote-address range { *start_ip_address* | *start_ip_address/mask* } to { *end_ip_address* | *end_ip_address/mask* }

Important: In StarOS 9.0 and later releases this keyword has been deprecated.

range specifies a range of IPv4/IPv6 addresses.
start_ip_address and *end_ip_address* specify, for the range, the starting and ending IPv4/IPv6 addresses.*end_ip_address* must be greater than *start_ip_address*.
start_ip_address/mask and *end_ip_address/mask* specify, for the range, the starting and ending IPv4/IPv6 address, and the number of subnet bits representing the subnet mask in shorthand.
end_ip_address/mask must be greater than *start_ip_address/mask*.

Usage

Use this command to configure the remote address(es) for a packet filter.

Example

The following command configures the IP remote address as *10.2.3.4/24*:

```
ip remote-address 10.2.3.4/24
```

ip remote-port

This command allows you to configure the IP remote port(s) for the current packet filter.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

ip remote-port { = *port_number* | range *start_port_number* to *end_port_number* }

no ip remote-port

no

If previously configured, deletes the ip remote-port configuration from the current packet filter.

port_number

Specifies the port number of the transport protocol.
port_number must be the port number, and must be an integer from 1 through 65535.

range *start_port_number* **to** *end_port_number*

Specifies a range of port numbers.
start_port_number and *end_port_number* must be integers from 1 through 65535.
end_port_number must be greater than *start_port_number*.

Usage

Use this command to configure the IP remote port(s) for a packet filter.

Example

The following command configures the IP remote port as *789*:

```
ip remote-port = 789
```

priority

This command allows you to configure the current packet filter's priority.

Important: This command is deprecated in certain 9.0 releases and in 10.0 and later releases. The precedence values of packet filters (those from both dynamic and predefined rules) are assigned by the PCEF based on an internal process.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

priority *priority*

no priority

no

If previously configured, deletes the priority configuration in the current packet filter.

priority

Specifies this packet filter's priority
priority must be an integer from 0 through 255.

Usage

Use this command to configure the packet filter's priority. The priority must be configured for the packet filter to be used in a TFT. Packets are compared against packet filters in a prioritized fashion, with 0 being the highest priority. Without this setting, this filter will not be used.

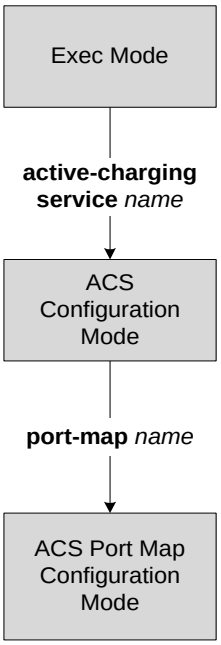
Example

The following command configures the packet filter's priority as *3*:

```
priority 3
```

Chapter 15
ACS Port Map Configuration Mode Commands

The ACS Port Map Configuration Mode is used to define an application-port mapping in the ACS Configuration Mode. The application-port map associates a range of ports to a specific application/protocol within a rule definition (ruledef).



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

port

This command allows you to add/remove an individual or a range of port numbers associated with an application or protocol from the current port map.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] port { *port_number* **| range** *start_port_number* **to** *end_port_number* **}**

no

If added previously, removes the specified port(s) from the current port map.

port_number

Specifies a port number to add to the current port map.
port_number must be a port number, and must be an integer from 1 through 65535.

range *start_port_number* **to** *end_port_number*

Specifies a range of port numbers to add to the current port map.
start_port_number specifies the starting port number of the range, it must be an integer from 1 through 65535, and must be less than *end_port_number*.
end_port_number specifies the ending port number of the range, it must be an integer from 1 through 65535, and must be greater than *start_port_number*.

Usage

Use this command to add an individual or a range of port numbers to a port map. Up to 10 sets of ports can be configured in each port map.

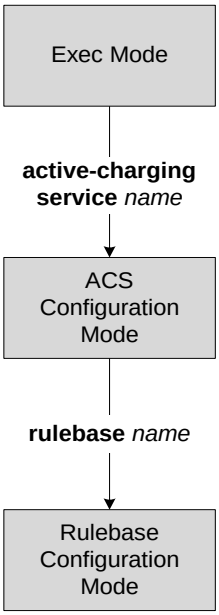
Example

The following command adds all port numbers from *3112* through *5000* to the port map:

```
port range 3112 to 5000
```

Chapter 16
ACS Rulebase Configuration Mode Commands

The ACS Rulebase Configuration Mode is used to configure Active Charging Service (ACS) rulebases.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

action priority

This command allows you to configure the action priority for a ruledef / group-of-ruledefs in the current rulebase.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

action priority *action_priority* **{ [dynamic-only | static-and-dynamic | timedef** *timedef_name* **] { group-of-ruledefs** *ruledefs_group_name* **| ruledef** *ruledef_name* **} charging-action** *charging_action_name* **[monitoring-key** *monitoring_key* **] [description** *description* **] }**

no action priority *action_priority*

no

If previously configured, deletes the specified action priority configuration from the current rulebase.

priority *action_priority*

Specifies a priority for the specified ruledef / group-of-ruledefs in the current rulebase.
action_priority must be unique in the current rulebase, and must be an integer from 1 through 65535. The priority controls the order in which this instance of the CLI command will be examined. Lower numbered priorities are examined first. Up to 2048 instances may be configured, totaled among all rulebases.

dynamic-only

Enables matching of dynamic rules with static rules for this action priority on a flow.
Configuring the **dynamic-only** keyword causes the configuration to be defined, but not enabled. If enabled, the action associated with this option will not be matched against a flow until it is enabled from a dynamic charging interface like Gx. Gx can disable or enable this action entry in the rulebase using Gx messages.
Default: Disabled

static-and-dynamic

The static-and-dynamic option causes the configuration to be defined and enabled, and allows a dynamic protocol (such as the Gx interface) to disable or re-enable the configuration.
Default: Enabled

Important: When R7 Gx is enabled, “static-and-dynamic” rules behave exactly like “dynamic-only” rules. That is, they must be activated explicitly by the Policy and Charging Rules Function (PCRF). When Gx is not enabled, “static-and-dynamic” rules behave exactly like static rules.

timedef *timedef_name*

Important: This keyword is only available in StarOS 8.1 and StarOS 9.0 and later releases.

Associates the specified time definition with the ruledef / group-of-ruledefs. Timedefs activate or deactivate ruledefs / groups-of-ruledefs, making them available for rule matching only when they are active.
timedef_name must be the name of a timedef, and must be an alphanumeric string of 1 through 63 characters.
A timedef can be used with several ruledefs / group-of-ruledefs. When a packet is received, and a ruledef / group-of-ruledefs is eligible for rule matching, if a timedef is associated with the ruledef / group-of-ruledefs, before rule matching the packet-arrival time is compared with the timeslots configured in the timedef. If the packet arrived in any of the timeslots configured in the associated timedef, rule matching is undertaken, else the next ruledef / group-of-ruledefs is considered.

Important: The time considered for timedef matching is the system's local time.

ruledef *ruledef_name*

Adds the specified ruledef to the current rulebase.
ruledef_name must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.
If the specified ruledef does not exist, there will be no ruledef triggers for this action priority within the current rulebase.

Important: If the ruledef specified here is deleted or is not configured, the system accepts it without applying any ruledef under current rulebase for this action priority.

group-of-ruledefs *ruledefs_group_name*

Adds the specified group-of-ruledefs to the current rulebase.
ruledefs_group_name must be the name of a group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.
When a group-of-ruledefs is specified, if any of the ruledefs within the group matches, the specified charging-action is applied, any more of the action instances are not processed.

Important: If the group-of-ruledefs specified here is deleted or is not configured, the system accepts it without applying any ruledefs under current rulebase for this action priority.

charging-action *charging_action_name*

Specifies the charging action.
charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.
If the specified charging action does not exist, there will be no charging action triggers for this action priority within the current rulebase.

Important: If the charging action specified here is not configured or is later deleted, the system will not apply any charging action under current rulebase for this action priority.

monitoring-key *monitoring_key*

Associates the specified monitoring-key with ruledefs for usage monitoring.
monitoring_key must be an integer from 1 through 4000000000.

description *description*

Adds specified text to the rule and action.
description must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure action priorities for ruledefs / group-of-ruledefs in a rulebase.
This CLI command can be entered multiple times to specify multiple ruledefs and charging actions. The ruledefs are examined in priority order, until a match is found and the corresponding charging action is applied.

Example

The following command assigns a rule and action with the action priority of *23*, a ruledef named *test*, and a charging action named *test1* to the current rulebase:

```
action priority 23 ruledef test charging-action test1
```

active-charging rf

This command allows you to enforce default rating group / service identifier on all PCC rules, predefined ACS rules, and static ACS rules for Rf-based accounting.

Important: This command is customer specific. For more information contact your Cisco account representative.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

active-charging rf { rating-group-override *rating_group* **| service-id-override** *service_id* **}**

{ default | no } active-charging rf { rating-group-override | service-id-override }

default

Configures this command with its default setting.
Default: Override configuration is disabled; same as no.

no

Disables the override configuration.
no active-charging rf rating-group-override: Rating group override will not be enforced on the PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own rating group, it will continue to use that.
no active-charging rf service-id-override: Service ID override will not be enforced on the PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own service ID, it will continue to use that.

rating-group-override *rating_group*

Enforces the specified rating group on all PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own rating group, it will be overridden by the specified rating group.
rating_group must be an integer from 1 through 65535.

service-id-override *service_id*

Enforces the specified service ID on all PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own service ID, it will be overridden by the specified service ID.
service_id must be an integer from 1 through 65535.

Usage

Use this command to enforce a specific rating group / service identifier on all PCC rules, predefined ACS rules, and static ACS rules for Rf-based accounting. As this CLI configuration is applied at the rulebase level, all the APNs that have the current rulebase defined will inherit the configuration.

Example

The following command configures the service ID *100*:

```
active-charging rf service-id-override 100
```

bandwidth default-policy

This command allows you to configure the default bandwidth policy for the current rulebase.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

bandwidth default-policy *bandwidth_policy_name*

no bandwidth default-policy

no

If previously configured, deletes the bandwidth default-policy configuration from the current rulebase.

bandwidth_policy_name

Specifies the default bandwidth policy for the current rulebase.
bandwidth_policy_name must be the name of a bandwidth policy, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the default bandwidth policy for a rulebase.
For subscribers using the current rulebase, the default bandwidth policy will be used if in the APN/subscriber profile the **default active-charging bandwidth-policy** command is configured, or no bandwidth policy is configured.

Example

The following command configures a bandwidth policy named *standard* for the rulebase:

```
bandwidth default-policy standard
```

billing-records

This command allows you to configure the type of billing to be performed for subscriber sessions.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
billing-records { egcdr | radius | rf | udr udr-format udr_format_name [ failure-
handling-udr-format udr_format_name ] } +

no billing-records
```

no

If previously configured, deletes the billing-records configuration from the current rulebase.

egcdr

Generates an enhanced G-CDR (eG-CDR) for GGSN / P-GW-CDR for P-GW, and/or UDR with specified format on the occurrence of an interim trigger condition at the end of a subscriber session, or an SGSN-to-SGSN handoff.

radius

Generates postpaid RADIUS accounting records at the start and end of a subscriber session, and on the occurrence of an interim trigger condition. RADIUS accounting records are generated for each content ID.

Important: In the GGSN, if in the APN configuration the "accounting-mode" is set to "none", the system continues to send ACS-generated RADIUS accounting messages. In the PDSN, if in the subscriber default configuration the "accounting-mode" is set to "none", the system does not send any RADIUS accounting messages (including ACS accounting messages).

rf

Enables Rf accounting.
Rf accounting is applicable only for dynamic and predefined rules that are marked for it. Dynamic rules have a field offline-enabled to indicate this. To mark a predefined rule as offline-enabled, use this keyword and the **billing-action** command in the ACS Charging Action Configuration Mode.

udr udr-format *udr_format_name*

Generates UDRs with specified the format on the occurrence of an interim trigger condition, at the end of a subscriber session, or a handoff.
udr_format_name must be the name of an UDR format, and must be an alphanumeric string of 1 through 63 characters.

+

Indicates that more than one of the keywords can be entered in a single command.

Usage

Use this command to generate enhanced G-CDRs (eG-CDRs), P-GW-CDR for P-GW, RADIUS CDRs and/or UDRs for billing records. The format of eG-CDRs for the default GTPP group is controlled by the **inspector** command in the Context Configuration Mode.
If, in the APN configuration, the "accounting-mode" is set as default (GTPP), and in the rulebase configuration "billing-records egcdr" is configured, both G-CDRs and eG-CDRs are generated if configured.
If, in the APN, the accounting-mode is set to "none" G-CDRs will not be generated.

Example

The following command sets the billing record to UDR with UDR format named *udr_format1*:

```
billing-records udr udr-format udr_format1
```

cca diameter requested-service-unit

This command allows you to specify the Diameter sub-AVPs to be included in the Diameter group AVP "Requested-Service-Unit" sent with DCCA Credit Control Requests (CCRs).

Product

All

Privilege

Security Administrator, Administrator

Syntax

cca diameter requested-service-unit sub-avp { time cc-time *duration* **| units cc-service-specific-units** *charging_unit* **| volume { cc-input-octets** *bytes* **| cc-output-octets** *bytes* **| cc-total-octets** *bytes* **} + }**

no cca diameter requested-service-unit sub-avp

no

No sub-AVPs are included in the Requested-Service-Unit grouped AVP.

time cc-time *duration*

Specifies requested service unit for charging time duration in seconds in included sub-AVP.
duration specifies charging time in seconds, and must be an integer from 1 through 4000000000.

units cc-service-specific-units *charging_unit*

Specifies requested service unit by service specific units in bytes/packets in included sub-AVP.
charging_unit specifies service-specific charging unit and must be an integer from 1 through 4000000000.

volume { cc-input-octets *bytes* **| cc-output-octets** *bytes* **| cc-total-octets** *bytes* **} +**

Specifies requested service unit for charging octets by input, output, and total volume in included sub AVP.

- **cc-input-octets**: Specifies input charging octets.
- **cc-output-octets**: Specifies output charging octets.
- **cc-total-octets**: Specifies total charging octets.
- *bytes*: Specifies volume in bytes and must be an integer from 1 through 4000000000.

+: Indicates that more than one of the previous keywords can be entered within a single command.

Usage

Use this command to include sub-AVPs based on time, volume, and service specific unit in the "Requested-Service-Unit" grouped AVP with CCRs through Gy interface.

Example

The following command sets the time based sub-AVP with charging duration of 45 seconds in "Requested-Service-Unit" group AVP on DCCA CCRs:

```
cca diameter requested-service-unit sub-avp time cc-time 45
```

cca quota

This command allows you to configure various time- and threshold-based quotas in the Prepaid Credit Control Service (Credit Control Application).

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
cca quota { holding-time holding_time content-id content_id | retry-time retry_time [
max-retries retries ] }

{ default | no } cca quota { holding-time content-id content_id | retry-time }
```

holding-time *holding_time*

Specifies the value for the Quota Holding Time (QHT). QHT is used with both time-based and volume-based quotas. After *holding_time* seconds has passed without user traffic, the quota is reported back and the charging stops until new traffic starts.
holding_time must be an integer from 1 through 4000000000.

content-id *content_id*

Specifies the content ID (Rating group AVP) to use for the Quota holding time for the current rulebase.
content_id is the content ID specified for credit control service in ACS.
In 12.1 and earlier releases, *content_id* must be an integer from 1 through 65535.
In 12.2 and later releases, *content_id* must be an integer from 1 through 2147483647.

retry-time *retry_time* **[max-retries** *retries* **]**

Specifies the retry time for the quota request, in seconds.
retry_time must be an integer from 0 through 86400. To disable this assign 0.
Default: 60
This parameter defines the maximum frequency at which the Credit-Control Application (CCA) tries to obtain quota for a subscriber passing traffic for a category with no/exhausted quota.
For a subscriber not passing traffic, the CCA will not try to obtain quota (except once at session start time, if so configured). The quota request from the no quota state is sent in response to user packets only (never based on a timer).
When subscriber hits a charging action that is a flow redirect, the operator can optionally specify that this redirection shall clear the retry-time timer.
This allows the immediately following chargeable user traffic to trip a quota request, even if it would otherwise have been subject to the retry time limit. Such configuration allows quite a large value for retry-time in quota charging or a top-up scenario.
max-retries *retries* configures the maximum number of retries allowed for blacklisted categories. This option has a default value of 65535 retries (the maximum value).
retries must be an integer from 1 through 65535. To disable this assign 0.

Usage

Use this command to set the prepaid credit control quotas.

cca quota retry time allows an operator to set the amount of time that the ACS waits before it retries the prepaid server for a content ID for which quota was exhausted earlier.

When the server sends the quota holding time (QHT) it has highest priority to use that QHT regardless of the value configured in the rulebase or Credit Control Application Configuration Mode. QHT configured here has the second priority for the content ID (rating group) configured here.

If the QHT is not available from the server or rulebase configuration mode, the QHT values configured via the Credit Control Application Configuration Mode are used.

Example

The following command configures the prepaid credit control request retry time to *30* seconds:

```
cca quota retry-time 30
```

The following command specifies the system to use the QHT value configured in the Credit Control Application Mode:

```
no cca quota holding-time content-id 1
```

The following command specifies the system to ignore the QHT value configured in the Credit Control Application Mode:

```
default cca quota holding-time content-id 1
```

The following command configures the prepaid credit control request retry time to *60* seconds and the maximum number of retries to *65535*:

```
default cca quota retry-time max-retries
```

cca quota time-duration algorithm

This command allows you to specify the algorithm to compute time duration for Prepaid Credit Control Application quotas in the current rulebase.

Product

All

Privilege

Security Administrator, Administrator

Syntax

cca quota time-duration algorithm { consumed-time *seconds* **[plus-idle] | continuous-time-periods** *seconds* **| parking-meter** *seconds* **} [content-id** *content_id* **]**

default cca quota time-duration algorithm

no cca quota time-duration algorithm { consumed-time | continuous-time-periods | parking-meter } [content-id *content_id* **]**

no

If previously configured, deletes the quota time-duration algorithm configuration from the current rulebase.

default

Configures this command with its default setting.

consumed-time *seconds*

Specifies the Quota Consumption Time (QCT) in seconds. QCT is used with active time-based quotas and to determine chargeable time envelopes for consuming time quota.
seconds must be an integer from 1 through 4294967295.
Default: 0 (disabled)
A time envelope is the basis for reporting active usage. For each time envelope, the quota consumption includes the last QCT (duration between first packet and last packet + QCT).

plus-idle

Specifies the idle time for QCT.
When used along with **consumed-time** it indicates the active usage + idle time, when no traffic flow occurs.

continuous-time-periods *seconds*

Specifies the charging quota continuous period, in seconds.
seconds must be an integer from 1 through 4294967295.
Default: 0 (disabled)
The Continuous Time Periods (CTP) mechanism constructs time-envelopes from consecutive base time intervals in which traffic has occurred up to and including a base time interval which contains no traffic. As with Quota-Consumption-Time envelopes, the end of an envelope can only be determined “retrospectively”. Again, as with Quota-Consumption-Time, the envelope for CTP includes the last base time interval (the one which contained no traffic).

parking-meter *seconds*

Specifies the Parking Meter (PM) period, in seconds, for a particular rating group.
seconds must be an integer from 1 through 4294967295.
Default: 0 (disabled)
This mechanisms utilizes time quota, but instead of consuming linearly—once a decision to consume has been taken—the granted quota is consumed discretely in "chunks" of the base time interval at the start of each base time interval. Traffic is then allowed to flow for the period of the consumed quota.
The time interval seconds defines the length of the Parking Meter. A time-envelope corresponds to exactly one PM (and thus to one base time interval).

content-id *content_id*

Specifies the content ID (Rating group AVP) to use for the CCA Quota time duration algorithm selection in the current rulebase.
content_id is the content ID specified for credit control service in ACS,
In 12.1 and earlier releases, *content_id* must be an integer from 1 through 65535.
In 12.2 and later releases, *content_id* must be an integer from 1 through 2147483647.

Usage

Use this command to set the various time charging algorithms/schemes for prepaid credit control charging. If operator chooses **parking-meter** *seconds* style charging, then time is billed in *seconds* chunks.

Example

The following command configures the QCT to consumed-time duration of *400* seconds:

```
cca quota time-duration algorithm consumed-time 400
```

cca radius accounting interval

This command allows you to configure how often interim updates are generated by the RADIUS Credit Control Application to be sent to the prepaid server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

cca radius accounting interval *interval*

{ default | no } cca radius accounting interval

default

Configures the command with its default setting.
Default: Disabled; same as **no cca radius accounting interval**

no

Disables interim updates.

interval

Specifies the time interval, in seconds, between interim updates generated by the RADIUS Credit Control Application.
interval must be an integer from 1 through 3600.
Default: 1 (Disabled)

Usage

Use this command to specify the RADIUS accounting interval between accounting of a prepaid subscriber. The same parameters are applicable for RADIUS server group.

Example

The following command defines RADIUS accounting interval of *20* seconds for RADIUS prepaid service in the rulebase:

```
cca radius accounting interval 20
```

cca radius charging context

This command allows you to specify the RADIUS servers used for the current rulebase when RADIUS credit control is enabled.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

cca radius charging context *vpn_context* **[group** *server_group_name* **]**

no cca radius charging context

no

RADIUS credit control will not be performed.

vpn_context

Specifies the charging context where RADIUS prepaid charging parameters are configured.
vpn_context must be an alphanumeric string of 1 through 79 characters.

group *server_group_name*

Specifies the RADIUS server group.
server_group_name must be the name of a RADIUS server group, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify the RADIUS charging context where RADIUS prepaid charging parameters are configured. The same parameters are applicable for RADIUS server group.

Example

The following command defines RADIUS charging context *prepaid_rad1* for RADIUS prepaid charging in the rulebase:

```
cca radius charging context prepaid_rad1
```

cca radius user-password

This command allows you to configure the value to use for the "User-Password" attribute in RADIUS messages sent to the prepaid server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

cca radius user-password [encrypted] password *password*

no cca radius user-password

no

If previously configured, deletes the RADIUS prepaid service user password configured in the current rulebase.

[encrypted] password *password*

Specifies the password for prepaid services within the current rulebase.
In 12.1 and earlier releases, *password* must be an alphanumeric string of 1 through 63 characters with or without encryption.
In 12.2 and later releases, *password* must be an alphanumeric string of 1 through 63 characters without encryption, and 1 through 132 characters with encryption enabled.
The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

Usage

Use this command to specify the RADIUS user password for prepaid services within the current rulebase.

Example

The following command configures the user password as *user_123* without encryption in the current rulebase:

```
cca radius user-password password user_123
```

charging-rule-optimization

This command allows you to configure the internal optimization level to use, for improved performance, when evaluating each instance of the **action priority** command.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
charging-rule-optimization { high | low | medium }

default charging-rule-optimization
```

default

Configures this command with its default setting.
Default: In 10.0 and earlier releases: **low**. In 11.0 and later releases: **high**

high

Enables the highest level of optimization with high memory utilization.

low

Enables minimal level of optimization with minimal memory utilization.

medium

Important: In 11.0 and later releases, the **medium** keyword is deprecated.

Enables medium level of optimization with moderate memory utilization.

Usage

Use this command to specify the level of internal optimization for improved performance when evaluating each instance of the **action priority** command.
Both the high and medium options cause re-organization of the entire memory structure whenever any change is made, such as on the addition of an **action prority** command.

Example

The following command specifies the highest optimization level for rule search and matching in the rulebase:

```
charging-rule-optimization high
```

constituent-policies

This command allows you to configure the Bandwidth, Content Based Billing (CBB), and Firewall/Firewall-and-NAT constituent policies. The combination of the values of all three policies will uniquely identify the associated rulebase.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
constituent-policies { bandwidth-policy bandwidth_policy_name | cbb-policy
cbb_policy_name | firewall-policy fw_policy_name | fw-and-nat-policy fw_nat_policy_name }
+

no constituent-policies
```

no

If previously configured, deletes the constituent-policies configuration from the current rulebase.

bandwidth-policy *bandwidth_policy_name*

Specifies the Bandwidth policy.
bandwidth_policy_name must be the name of a bandwidth policy, and must be an alphanumeric string of 1 through 63 characters.

cbb-policy *cbb_policy_name*

Specifies the Content Based Billing (CBB) policy.
cbb_policy_name must be the name of a CBB policy, and must be an alphanumeric string of 1 through 63 characters.

firewall-policy *fw_policy_name*

Important: This keyword is customer specific. For more information, please contact your Cisco account representative.

Specifies the Stateful Firewall policy.
fw_policy_name must be the name of a Stateful Firewall policy, and must be an alphanumeric string of 1 through 63 characters.

fw-and-nat-policy *fw_nat_policy_name*

Important: This keyword is customer specific, and is only available in StarOS 8.1 and in StarOS 9.0 and later releases.

Specifies the Firewall-and-NAT policy.
fw_nat_policy_name must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the bandwidth, CBB, and Firewall/Firewall-and-NAT constituent policies that will identify the rulebase. The combination of the values of all three policies will uniquely identify the rulebase associated.

Example

The following command configures the constituent bandwidth policy named *test123*:

```
constituent-policies bandwidth-policy test123
```

content-filtering category policy-id

This command allows you to configure the Content Filtering Category Policy Identifier for Policy-based Content Filtering support in the current rulebase.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

content-filtering category policy-id *cf_policy_id*

no content-filtering category policy-id [*cf_policy_id* **]**

no

If previously configured, deletes the configuration from the current rulebase.
In StarOS 8.1 and later releases, optionally the policy ID can be specified. If the specified policy ID is invalid, or is not configured in the rulebase, an error message is displayed. If no policy ID is specified, whatever policy is configured, if any, is removed from the rulebase.

content-filtering category policy-id *cf_policy_id*

Configures the specified Content Filtering Category Policy in the current rulebase.
cf_policy_id must be the ID of an existing Content Filtering Category Policy, and must be an integer from 1 through 4294967295.

Important: If the specified Content Filtering Category Policy does not exist, all packets will be passed regardless of the categories/actions determined for such packets.

Important: The category policy ID that is configured using the **category policy-id** *cf_policy_id* command in the APN/Subscriber Configuration Mode prevails over this configuration.

Usage

Use this command to configure the Content Filtering Category Policy ID for Policy-based Content Filtering support in the rulebase.
The Content Filtering Category Policy is created/deleted in the ACS Configuration Mode, and is configured in the Content Filtering Policy Configuration Mode.

Example

The following command configures the Content Filtering Category Policy ID *101* in the rulebase:

```
content-filtering category policy-id 101
```

content-filtering flow-any-error

This command allows you to specify action to take on Content Filtering packets in the case of ACS error scenarios.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

```
content-filtering flow-any-error { deny | permit }

default content-filtering flow-any-error
```

default

Configures this command with its default setting.
Default: **permit**

deny

Configures flow-any-error configuration as deny.
All the denied packets will be accounted for by the **discarded-flow-content-id** configuration in the Content Filtering Policy Configuration Mode. This content ID will be used to generate UDRs for packets denied via content filtering.

permit

Configures flow-any-error configuration as permit.

Usage

Use this command to allow/discard content filtering packets in case of ACS error scenarios.

Example

The following command allows content filtering packets in case of an ACS error:

```
content-filtering flow-any-error permit
```

content-filtering mode

This command allows you to enable/disable the specified Category-based Content Filtering mode in the current rulebase.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

content-filtering mode { category { static-and-dynamic | static-only } | server-group *cf_server_group* **}**

no content-filtering mode

---

no

If previously configured, deletes the content-filtering mode configuration from the current rulebase. Content filtering will not to be performed for the current rulebase. This is the default setting.

---

category { static-and-dynamic | static-only }

Specifies the Category-based Content Filtering mode.

- **static-only**: Configures Category-based Content Filtering in static only mode, wherein all URLs are compared against an internal database to categorize the requested content.

  Using Category-based Content Filtering support requires configuration of the **require active-charging content-filtering category** command in the Global Configuration Mode.

- **static-and-dynamic**: Configures Category-based Content Filtering in Static-and-Dynamic mode, wherein a static rating of the URL is first performed, and only if the static rating fails to find a match, dynamic rating of the content that the server returns is then performed.

Important: Before enabling static-and-dynamic rating in the rulebase, it must be enabled at the global level as the resources required for dynamic rating are allocated at the global level. To enable static-and-dynamic rating at the global level, in the Global Configuration Mode use the **require active-charging content-filtering category static-and-dynamic** command.

---

server-group *cf_server_group*

Enables and configures the Content Filtering Server Group (CFSG) mode within the rulebase to manage an external content filtering server with an Internet Content Adaptation Protocol (ICAP) client system.
cf_server_group must be the name of a CFSG, and must be unique, and must be an alphanumeric string of 1 through 63 characters.
If configured, ACS attempts to establish TCP connections to every server in the named group.

Usage

Use this command to enable and apply the content filtering mode in the rulebase to manage a content filtering server with an ICAP client system.

Example

The following command enables the content filtering mode for external content filtering server group *CF_Server1* in the rulebase:

```
content-filtering mode server-group CF_Server1
```

The following command enables the category based static and dynamic content filtering mode for in the rulebase:

```
content-filtering mode category static-and-dynamic
```

dynamic-rule order

This command allows you to specify whether dynamic rules are matched before statically configured rules.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
dynamic-rule order { always-first | first-if-tied }

no dynamic-rule order
```

no

If previously configured, deletes the dynamic-rule order configuration from the current rulebase. By default, dynamic rules are matched against the flow prior to static rules.

always-first

Specifies to match all the dynamic rules against the flow prior to any static rule.

first-if-tied

Specifies to match rules against the flow based on their priority with the condition that dynamic rules match before a static rule of the same priority.
A rule is a combination of a ruledef, charging action, and precedence. Static rules are defined by the **action** CLI command in the ACS Rulebase Configuration Mode, and are applicable to all subscribers that are associated with the rulebase. Dynamic rules are obtained via a dynamic protocol, such as, the Gx-interface for a particular subscriber session.

Usage

Use this command to configure the order in which rules are selected for matching in between dynamic rules (per subscriber) and static rules (from rulebase).

Example

The following command matches all dynamic rules against the flow prior to any static rule:

```
dynamic-rule order always-first
```

edr sn-charge-volume

This command allows you to exclude/include packets/bytes that are dropped/retransmitted by the ACS in the total charge volume — "sn-charge-volume" EDR attribute.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] edr sn-charge-volume { count-dropped-units | count-retransmitted-units }
```

default

Configures this command with its default setting.
Default: Exclude, in the total charge volume, packets/bytes dropped/retransmitted by ACS.

no

Exclude, in the total charge volume, packets/bytes dropped/retransmitted by ACS.

count-dropped-units

Specifies to include dropped units in the total charge volume.

count-retransmitted-units

Specifies to include retransmitted units in the total charge volume.

Usage

Use this command to exclude/include packets/bytes that are dropped/retransmitted by ACS in the total charge volume — "sn-charge-volume" EDR attribute.
This command applies only to the "sn-charge-volume" attribute and does not affect the "sn-volume-amt" counts in any way.

Example

The following specifies to include units retransmitted by ACS in the sn-charge-volume EDR attribute:

```
edr sn-charge-volume count-retransmitted-units
```

edr suppress-zero-byte-records

This command disables/enables the creation of EDRs when there is no data for the flows.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[default | no] edr suppress-zero-byte-records

default

Configures this command with its default setting.
Default: Disabled; same as **no edr suppress-zero-byte-records**

no

Disables the suppression of zero-byte EDRs.

edr suppress-zero-byte-records

Suppresses zero-byte EDRs.

Usage

Use this command to disable/enable the creation of EDRs that are empty. The situation where there is a zero-byte EDR would typically be possible when two successive EDRs are generated for a flow. This CLI command suppresses the second such EDR for the flow.

edr transaction-complete

This command enables/disables the generation of an EDR on the completion of a transaction.

Important: This command is available only in StarOS 8.1 and in StarOS 9.0 and later releases.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

In 12.1 and earlier releases:

edr transaction-complete http edr-format *edr_format_name*

{ default | no } edr transaction-complete

In 12.2 and later releases:

edr transaction-complete http [charging-edr *charging_edr_format_name* **| edr-format** *edr_format_name* **| reporting-edr** *reporting_edr_format_name* **]**

{ default | no } edr transaction-complete

default

Configures this command with its default setting.
Default: Disabled; same as **no edr transaction-complete**

no

If previously configured, deletes the configuration from the current rulebase.

edr-format *edr_format_name*

Important: This option is available only in 12.1 and earlier releases. In 12.2 and later releases, this option is deprecated and is replaced by the **charging-edr** option.

Specifies to generate EDR on transaction completion, for HTTP protocol.
edr_format_name must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.

charging-edr *charging_edr_format_name*

Important: This option is available only in 12.2 and later releases.

Specifies to generate charging EDR on transaction completion.

charging_edr_format_name must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

reporting-edr *reporting_edr_format_name*

Important: This option is available only in 12.2 and later releases.

Specifies to generate reporting EDR on transaction completion.
reporting_edr_format_name must be the name of a reporting EDR, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the generation of an EDR when certain application transactions (for example, request/response pairs) complete. In this release EDR generation is supported only for HTTP protocol. Note that these EDRs are in addition to those that might be generated due to other conditions, for example, EDR configurations in a Charging Action.

Example

In 12.1 and earlier releases, the following command configures the generation of EDRs on the completion of transactions for HTTP protocol specifying the EDR format as *test123*:

```
edr transaction-complete http edr-format test123
```

In 12.2 and later releases, the following command configures the generation of charging EDRs on the completion of transactions for HTTP protocol specifying the EDR format as *test123*:

```
edr transaction-complete http charging-edr test123
```

edr voip-call-end

This command enables/disables generation of EDRs on the completion of Voice over IP (VoIP) calls.

Product

ACS, ADC

Privilege

Security Administrator, Administrator

Syntax

In 12.1 and earlier releases:

```
edr voip-call-end edr-format edr_format_name

{ default | no } edr voip-call-end
```

In 12.2 and later releases:

```
edr voip-call-end { charging-edr charging_edr_format_name | edr-format edr_format_name |
reporting-edr reporting_edr_format_name } +

{ default | no } edr voip-call-end
```

default

Configures this command with its default setting.
Default: Disabled; same as **no edr voip-call-end**

no

If previously configured, deletes the edr voip-call-end configuration from the current rulebase.

edr-format *edr_format_name*

Important: This option is available only in 12.1 and earlier releases. In 12.2 and later releases, it has been deprecated and is replaced by the **charging-edr** option.

Specifies to generate an EDR when a VoIP call ends.
edr_format_name must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.

charging-edr *charging_edr_format_name*

Important: This option is available only in 12.2 and later releases.

Specifies to generate a charging EDR when a VoIP call ends.
charging_edr_format_name must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

reporting-edr *reporting_edr_format_name*

Important: This option is available only in 12.2 and later releases.

Specifies to generate a reporting EDR when a VoIP call ends.
reporting_edr_format_name must be the name of a reporting EDR format, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to generate an EDR on the completion of voice calls. Note that these EDRs are in addition to those that might be generated due to other conditions, for example EDR configurations in a Charging Action. This command facilitates P2P voice duration reporting.

Example

In 12.1 and earlier releases, the following command specifies generating EDRs on completion of VoIP calls using the EDR format *test13*:

```
edr voip-call-end edr-format test13
```

In 12.2 and later releases, the following command specifies generating charging EDRs on completion of VoIP calls using the EDR format named *test23*:

```
edr voip-call-end charging-edr test23
```

egcdr inactivity-meter

Description This command has been deprecated. It is included in the CLI for backward compatibility with older configuration files. When executed performs no function. Use the **egcdr threshold interval** *interval* **[regardless-of-other-triggers]** command for this functionality.

egcdr cdr-encoding

This command allows you to configure the eG-CDR encoding type.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
egcdr cdr-encoding { ascii [ delimiter { colon | comma | pipe } ] | asn.1 }

default egcdr cdr-encoding
```

default

Configures the default eG-CDR CDR-encoding format.
Default: **asn.1**

ascii [delimiter { colon | comma | pipe }]

Specifies to use ASCII encoding type to generate eG-CDR in ASCII format.
delimiter { colon | comma | pipe }: Specifies the delimiter character to use in eG-CDRs in ASCII format.

- **colon**: Specifies to use ":" (colon) as a delimiter in eG-CDR.
- **comma**: Specifies to use "," (comma), as a delimiter in eG-CDR.
- **pipe**: Specifies to use "|" (pipe) as a delimiter in eG-CDR.

Default: **pipe**

asn.1

Specifies to use ASN.1 encoding type to generate eG-CDR in ASN.1 format.
This is the default setting.

Usage

Use this command to configure the eG-CDR encoding type.
For more information on using eG-CDR ASCII encoding type in your deployment, contact your Cisco account representative.

Example

The following command specifies to use ASCII encoding type to generate eG-CDR in ASCII format while specifying the delimiter character as comma:

```
egcdr cdr-encoding ascii delimiter comma
```

egcdr tariff

This command allows you to configure the eG-CDR tariff time to generate new eG-CDRs for GGSN and P-GW-CDRs for P-GW.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

[no] egcdr tariff minute *minute* **hour** *hour*

no

If previously configured, deletes the configuration from the current rulebase.

minute *minute*

Specifies the minute for the time-of-day configuration.
minute must be an integer from 0 through 59.

hour *hour*

Specifies the hour for the time-of-day configuration.
hour must be an integer from 0 through 23.

Usage

Use this command to configure the eG-CDR tariff time to generate new eG-CDRs for GGSN and P-GW-CDRs for P-GW. Up to four different time-of-day settings may be configured. When any configured tariff time is reached, the current eG-CDR/P-GW-CDR will be closed and a new eG-CDR/P-GW-CDR is opened.

Example

The following command defines an eG-CDR tariff for the 23rd minute of the 22nd hour of the day (10:23 PM):

```
egcdr tariff minute 23 hour 22
```

egcdr threshold

This command allows you to configure the thresholds for generating eG-CDRs for GGSN and P-GW-CDRs for P-GW.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

egcdr threshold { interval *interval* **[regardless-of-other-triggers] | volume { downlink | total | uplink }** *bytes* **}**

{ default | no } egcdr threshold { interval | volume }

---

no

If previously configured, deletes the eG-CDR threshold configuration from the current rulebase.

---

default

Configures this command with the default settings.
Default: Disabled; same as **no egcdr threshold interval** and **no egcdr threshold interval volume** commands.

---

interval *interval* **[regardless-of-other-triggers]**

Specifies the time interval, in seconds, for closing the eG-CDR/P-GW-CDR if the minimum time duration thresholds are satisfied.
interval must be an integer from 60 through 40000000.
regardless-of-other-triggers: This option enables eG-CDR/P-GW-CDR generation at the fixed time interval irrespective of any other eG-CDR/P-GW-CDR triggers that may have happened in between.
Default: Disabled.

---

volume { downlink | total | uplink } *bytes*

Specifies the uplink/downlink volume octet counts for the generation of the interim eG-CDRs/P-GW-CDRs.

- **downlink** *bytes*: Specifies the limit for the number of downlink (from network to subscriber) octets after which the eG-CDR/P-GW-CDR is closed.

  bytes must be an integer from 100000 through 4000000000.

  Default: 4000000000

- **total** *bytes*: Specifies the limit for the total number of octets (uplink+downlink) after which the eG-CDR/P-GW-CDR is closed.

  bytes must be an integer from 100000 through 4000000000.

  Default: Disabled

- **uplink** *bytes*: Specifies the limit for the number of uplink (from subscriber to network) octets after which the eG-CDR/P-GW-CDR is closed.

  bytes must be an integer from 100000 through 4000000000.

  Default: 4000000000

Usage

Use this command to configure thresholds to generate eG-CDRs/P-GW-CDRs.

Thresholds can be specified for both time interval and for data volume, by entering the command twice (once with interval and once with volume). When either configured threshold is reached, the eG-CDR/P-GW-CDRs will be closed. The volume trigger can be specified for uplink or downlink or combined total (uplink + downlink) byte thresholds. The exact keyword forces the configured volume to exactly match the volume in the eG-CDR/P-GW-CDRs, so the triggering packet might have to be divided across two eG-CDRs/P-GW-CDRs.

When both interval and volume triggers are configured, we'll reset the interval time and accumulated volume amount whenever the eG-CDR/P-GW-CDRs is closed regardless of whether it was due to the interval time expiration or reaching the volume limit. Use the regardless-of-other-triggers optional keyword, if you want the eG-CDRs/P-GW-CDRs closed at the configured regular intervals, regardless of whether eG-CDRs/P-GW-CDRs are being closed due to reaching a volume limit.

When the PDP context is terminated, the eG-CDR/P-GW-CDRs will be closed regardless of whether the thresholds have been reached.

Example

The following command defines an eG-CDR threshold interval of *600* seconds:

```
egcdr threshold interval 600
```

egcdr time-duration algorithm

This command allows you to specify the algorithm to compute the duration of time utilization in an eG-CDR for the current rulebase.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

egcdr time-duration algorithm { consumed-time *consumed_time* **[plus-idle] | continuous-time-periods** *ctp_time* **| parking-meter** *seconds* **}**

{ default | no } egcdr time-duration algorithm

no

If previously configured, deletes the eG-CDR time-duration algorithm configuration from the current rulebase.

default

Configures this command with its default setting.
Default: Algorithm configured for CCA, or the CCA default if none is configured.

consumed-time *consumed_time* **[plus-idle]**

Specifies the actual consumption time in seconds. This is used to determine the actual used chargeable time envelopes for the purpose of consuming time quota.
consumed_time must be an integer from 1 through 4294967295.
Default: 0 (disabled)
Time envelope is the basis for reporting active usage. For each time envelope, the time consumption includes the time duration between arrival of last packet and first packet only.
plus-idle: Specifies the idle time between arrival of two packets to include in time usage record in eG-CDR.
When used along with **consumed-time** it indicates the active usage + idle time, when no traffic flow occurs.

continuous-time-periods *ctp_time*

Specifies the continuous time period to compute the usage record in eG-CDR.
ctp_time sets the audition, in seconds, to start a counter on arrival of the first packet and thereafter include only that period in charging in which one or more packets arrived. For the period where no packets arrived or no traffic was detected, usage will not be computed.
ctp_time must be an integer from 1 through 4294967295.

parking-meter *seconds*

Specifies the Parking Meter (PM) period, in seconds.
seconds must be an integer from 1 through 4294967295.
Parking meter is the method with which the usage time is set in the content-id containers in eG-CDRs. When a parking meter value is set, the user is charged for time in increments of the value set. For example, if the

parking meter is set to 300 seconds (5 minutes) and the subscriber only uses one minute, the charge is for 5 minutes.

Usage

Use this command to set the various time charging algorithms/schemes for time usage in eG-CDR.
For example, packets arrive at times T1, T2, T3 and T4. Then the typical time usage might be computed to be T4 – T1. However, if say there is an idle period between times T2 and T3, then system will compute the time usage to be (T2 – T1) + (T4 – T3).
consumed-time in above scenario calculates the time duration as (T2 – T1) + (T4 – T3) where **consumed-time** with **plus-idle** calculates the time duration as (T2-T1)+I + (T4 – T3)+I or (T4-T1).

Example

The following command sets consumed time duration to *400* seconds:

```
egcdr time-duration algorithm consumed-time 400
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

extract-host-from-uri

This command allows you to configure whether to use the host name embedded in the URI as the host field, when the host field option in the HTTP or Wireless Session Protocol (WSP) header is absent.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
extract-host-from-uri { http | wsp ) +

{ default | no } extract-host-from-uri
```

default

Configures this command with its default setting.
Default: Disabled; same as **no extract-host-from-uri**

no

If previously configured, disables the extract-host-from-uri configuration, for both HTPP and WSP, from the current rulebase.

http | wsp

Specifies the protocol(s).

+

Indicates that more than one of the previous keywords can be entered within a single command.

Usage

If the host field is not present in HTTP/WSP header, this command will extract host from the URI, and store it in the host field to enable “http host” and “wsp host” rule matches using the stored value.

Important: Applying the **extract-host-from-uri** command a second time will overwrite the previous configuration. For example, if you apply the command **extract-host-from-uri http wsp http**, and then apply the command **extract-host-from-uri http wsp**, extraction of host from URI will happen only for WSP analyzer.

Example

The following command configures extraction of host from URI for both HTTP and WSP protocols:

```
extract-host-from-uri http wsp
```

fair-usage session-waiver-percent

This command allows you to configure a waiver on top of average available memory credits per session for the Fair Usage feature.

Product

ACS, ADC, CF, FW, NAT

Privilege

Security Administrator, Administrator

Syntax

fair-usage session-waiver-percent *waiver_percent*

default fair-usage session-waiver-percent

default

Configures this command with its default setting.
Default: 20 percent

waiver_percent

Specifies the Fair Usage session waiver above average available memory for subscribers using the current rulebase.
waiver_percent must be an integer from 1 through 1000.
Default: 20 percent

Usage

Use this command to configure a waiver on top of average available memory credits per session at the rulebase level. That is, an allowance to use more than the average amount of memory.

Example

The following command configures the Fair Usage Session Waiver setting to *25*percent:

```
fair-usage session-waiver-percent 25
```

firewall dos-protection

This command allows you to configure Stateful Firewall protection for subscribers from Denial-of-Service (DoS) attacks.

Important: In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] firewall dos-protection { all | flooding { icmp | tcp-syn | udp } | ftp-bounce |
ip-unaligned-timestamp | mime-flood | port-scan | tcp-window-containment | source-router
| teardrop | winnuke }

default firewall dos-protection
```

no

If previously enabled, disables Stateful Firewall protection for subscribers from all or specified DoS attack(s).

default

Configures this command with its default setting.
Default: Protection from all DOS attacks is disabled.

all

Enables protection against all DoS attacks supported by the Stateful Firewall in-line service.

flooding { icmp | tcp-syn | udp }

Enables protection against specified flooding attacks:

- **icmp**: Enables protection against ICMP Flood attacks
- **tcp-syn**: Enables protection against TCP SYN Flood attacks
- **udp**: Enables protection against UDP Flood attacks

ftp-bounce

Enables protection against FTP Bounce attacks.
In an FTP Bounce attack, an attacker is able to use the PORT command to request access to ports indirectly through a user system as an agent for the request. This technique is used to port scan hosts discreetly, and to access specific ports that the attacker cannot access through a direct connection.

ip-unaligned-timestamp

Enables protection against IP Unaligned Timestamp attacks.
In an IP Unaligned Timestamp attack, certain operating systems crash if they receive a frame with the IP timestamp option that is not aligned on a 32-bit boundary.

mime-flood

Enables protection against HTTP Multiple Internet Mail Extension (MIME) Header Flooding attacks.
In a MIME Flood attack an attacker sends huge amount of MIME headers which consumes a lot of memory and CPU usage.

port-scan

Enables protection against Port Scan attacks.

tcp-window-containment

Enables protection against TCP Sequence Number Out-of-Range attacks.
In a Sequence Number Out-of-Range attack the attacker sends packets with out-of-range sequence numbers forcing the system to wait for missing sequence packets.

source-router

Enables protection against IP Source Route IP Option attacks.
Source routing is an IP option mainly used by network administrators to check connectivity. When an IP packet leaves a system, its path through various networks to its destination is controlled by the routers and their current configuration. Source routing provides a means to override the control of the routers. Strict source routing specifies the path through all the routers to the destination. The same path in reverse is used to return responses. Loose source routing allows the attacker to spoof both an address and sets the loose source routing option to force the response to return to the attacker's network.

teardrop

Enables protection against Teardrop attacks.
In a Teardrop attack, overlapping IP fragments are exploited causing the TCP/IP fragmentation re-assembly to improperly handle overlapping IP fragments.

winnuke

Enables protection against WIN-NUKE attacks.
This is a type of Nuke denial-of-service attack against networks consisting of fragmented or otherwise invalid ICMP packets sent to the target, achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop.
The WinNuke exploits the vulnerability in the NetBIOS handler and a string of out-of-band data sent to TCP port 139 of the victim machine causing it to lock up and display a Blue Screen of Death.

Usage

Use this command to enable Stateful Firewall protection from different types of DoS attacks. This command can be used multiple times for different DoS attacks.

Important: The DoS attacks are detected only in the downlink direction.

Example

The following command enables Stateful Firewall protection from all supported DoS attacks:

```
firewall dos-protection all
```

firewall flooding

This command allows you to configure Stateful Firewall protection from Packet Flooding attacks.

Important: In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit packets } | {
sampling-interval interval } }

default firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit } | {
sampling-interval } }
```

default

Configures this command the default setting for the specified keyword.

protocol { icmp | tcp-syn | udp }

Specifies the transport protocol:

- **icmp**: Configuration for ICMP protocol.
- **tcp-syn**: Configuration for TCP-SYN packet limit.
- **udp**: Configuration for UDP protocol.

packet limit *packets*

Specifies the maximum number of specified packets a subscriber can receive during a sampling interval.
packets must be an integer from 1 through 4294967295.
Default: 1000 packets per sampling interval for all protocols.

sampling-interval *interval*

Specifies the flooding sampling interval, in seconds.
interval must be an integer from 1 through 60.
Default: 1 second

Usage

Use this command to configure the maximum number of ICMP, TCP-SYN, / UDP packets allowed to prevent the packet flooding attacks to the host.

Example

The following command ensures a subscriber will not receive more that 1000 ICMP packets per sampling interval:

```
firewall flooding protocol icmp packet limit 1000
```

The following command ensures a subscriber will not receive more than 1000 UDP packets per sampling interval on different 5-tuples. That is, if an attacker is sending lot of UDP packets on different ports or using different spoofed IPs, those packets will be limited to 1000 packets per sampling interval. This way only "suspected" malicious packets are limited and not "legitimate" packets:

```
firewall flooding protocol udp packet limit 1000
```

The following command ensures a subscriber will not receive more than 1000 TCP-SYN packets per sampling interval:

```
firewall flooding protocol tcp-syn packet limi 1000
```

The following command specifies a flooding sampling interval of 1 second:

```
firewall flooding sampling-interval 1
```

firewall icmp-destination-unreachable-message-threshold

This command allows you to configure a threshold on the number of ICMP error messages sent by the subscriber for a particular data flow.

Important: In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall icmp-destination-unreachable-message-threshold *messages* **then-block-server**

{ default | no } firewall icmp-destination-unreachable-message-threshold

default

Configures this command with its default setting.
Default: No limit

no

If previously configured, deletes the configuration from the current rulebase.

messages

Specifies the threshold on the number of ICMP error messages sent by the subscriber for a particular data flow.
messages must be an integer from 1 through 100.

Usage

Use this command to configure a threshold on the number of ICMP error messages sent by the subscriber for a particular data flow. After the threshold is reached, it is assumed that the server is not reacting properly to the error messages, and further downlink traffic to the subscriber on the unwanted flow is blocked.
Some servers that run QChat ignore the ICMP error messages (Destination Port Unreachable and Host Unreachable) from the mobiles. So the mobiles continue to receive unwanted UDP traffic from the QChat servers, and their batteries get exhausted quickly.

Example

The following command configures a threshold of 10 ICMP error messages:

```
firewall icmp-destination-unreachable-message-threshold 10 then-block-
server
```

firewall max-ip-packet-size

This command allows you to configure the maximum IP packet size (after IP reassembly) allowed over Stateful Firewall.

Important: In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall max-ip-packet-size *packet_size* **protocol { icmp | non-icmp }**

default firewall max-ip-packet-size protocol { icmp | non-icmp }

default

Configures the default maximum IP packet size configuration.
Default: 65535 bytes (for both ICMP and non-ICMP)

packet_size

Specifies the maximum packet size.
packet_size must be an integer from 30000 through 65535.

protocol { icmp | non-icmp }

Specifies the transport protocol:

- **icmp**: Configuration for ICMP protocol.
- **non-icmp**: Configuration for protocols other than ICMP.

Usage

Use this command to configure the maximum IP packet size allowed for ICMP and non-ICMP packets to prevent packet flooding attacks to the host. Packets exceeding the configured size will be dropped for “Jolt Attack” and “Ping-Of-Death Attack”.

Example

The following command allows a maximum packet size of *60000* for ICMP protocol:

```
firewall max-ip-packet-size 60000 protocol icmp
```

firewall mime-flood

This command allows you to configure Stateful Firewall protection from Multipurpose Internet Mail Extensions (MIME) Flood attacks.

Important: In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall mime-flood { http-headers-limit *max_limit* **| max-http-header-field-size** *max_size* **}**

default firewall mime-flood { http-headers-limit | max-http-header-field-size }

default

Configures this command with its default setting.

http-headers-limit *max_limit*

Specifies the maximum number of headers allowed in an HTTP packet. If the number of HTTP headers in a page received is more than the specified limit, the request will be denied.
max_limit must be an integer from 1 through 256.
Default: 16

max-http-header-field-size *max_size*

Specifies the maximum header field size allowed in the HTTP header, in bytes. If the size of HTTP header in the received page is more than the specified number of bytes, the request will be denied.
max_size must be an integer from 1 through 8192.
Default: 4096 bytes

Usage

Use this command to configure the maximum number of headers allowed in an HTTP packet, and the maximum header field size allowed in the HTTP header to prevent MIME flooding attacks.

Example

The following command sets the maximum number of headers allowed in an HTTP packet to *100*:

```
firewall mime-flood http-headers-limit 100
```

The following command sets the maximum header field size allowed in the HTTP header to *1000* bytes:

```
firewall mime-flood max-http-header-field-size 1000
```

firewall no-ruledef-matches

This command allows you to configure the default action for packets when no Stateful Firewall ruledef matches.

Important: In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, use the **access-rule no-ruledef-matches** command available in the Firewall-and-NAT Policy Configuration Mode.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

firewall no-ruledef-matches { downlink | uplink } action { deny [charging-action *charging_action_name* **] | permit [bypass-nat | nat-realm** *nat_realm_name* **] }**

default firewall no-ruledef-matches { downlink | uplink } action

default

Configures the default action for packets with no Stateful Firewall ruledef match.

downlink | uplink

Specifies the packet type:

- **downlink**: Downlink (from network to subscriber) packets with no Stateful Firewall ruledef match.

  Default: **deny**

- **uplink**: Uplink (from subscriber to network) packets with no Stateful Firewall ruledef match.

  Default: **permit**

action { deny [charging-action *charging_action_name* **] | permit [bypass-nat | nat-realm** *nat_realm_name* **] }**

Specifies the default action for packets with no Stateful Firewall ruledef match.
permit [bypass-nat | nat-realm *nat_realm_name* **]**: Permit packets.

Important: The **bypass-nat** keyword is only available in StarOS 8.3 and later releases.

Optionally specify:

- **bypass-nat**: Specifies to bypass Network Address Translation (NAT).
- **nat-realm** *nat_realm_name*: Specifies a NAT realm to be used for performing NAT on subscriber packets.

  nat_realm_name must be the name of a NAT realm, and must be an alphanumeric string of 1 through 31 characters.

Important: If neither **bypass-nat** or **nat-realm** are configured, NAT is performed if the **nat policy nat-required** CLI command is configured with the **default-nat-realm** option.

deny [charging-action *charging_action_name* **]**: Denies specified packets.
Optionally, a charging action can be specified.
charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the default action to be taken on packets with no Stateful Firewall ruledef matches.
If, for deny action, the optional charging action is configured, the action taken depends on what is configured in the charging action. For the Stateful Firewall rule, the "flow action", "billing action", and "content ID" of the charging action will be used to take action. If flow exists, flow statistics are updated.
Allowing/dropping of packets is determined in the following sequence:

- Check is done to see if the packet matches any pinholes. If yes, no rule matching is done and the packet is allowed.
- Stateful Firewall ruledef matching is done. If a rule matches, the packet is allowed or dropped as per the **firewall priority** configuration.
- If no Stateful Firewall ruledef matches, the packet is allowed or dropped as per the **no-ruledef-matches** configuration.

For a packet dropped due to Stateful Firewall ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the **firewall priority** or the **firewall no-ruledef-matches** command respectively.
In StarOS 8.1, in the case of Policy-based Stateful Firewall, the charging action applied is the one configured in the **access-rule priority** or the **access-rule no-ruledef-matches** command respectively.
For action on packets dropped due to any error condition after data session is created, the charging action must be configured in the **flow any-error charging-action** command.

Example

The following command configures Stateful Firewall to permit downlink packets with no ruledef matches:

```
firewall no-ruledef-matches downlink action permit
```

firewall policy

This command allows you to enable/disable Stateful Firewall support for all subscribers using the current rulebase.

Important: In StarOS 8.0, this command is available in the APN/Subscriber Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
firewall policy firewall-required

{ default | no } firewall policy
```

default

Configures this command with its default setting.
Default: Stateful Firewall support is disabled for all subscribers using the current rulebase.

no

If previously enabled, disables Stateful Firewall support for all subscribers using the current rulebase.

firewall-required

Enables Stateful Firewall support for all subscribers using the current rulebase.

Usage

Use this command to enable/disable Stateful Firewall support for all subscribers using the current rulebase.

Example

The following command enables Stateful Firewall support:

```
firewall policy firewall-required
```

The following command disables Stateful Firewall support:

```
no firewall policy
```

firewall priority

This command allows you to add and specify the priority and type of a Stateful Firewall ruledef in the current rulebase, and allows you to configure a single or range of ports to be allowed on the server for auxiliary/data connections.

Important: In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, use the **access-rule priority** command available in the Firewall-and-NAT Policy Configuration Mode.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

firewall priority *priority* **[dynamic-only | static-and-dynamic] firewall-ruledef** *firewall_ruledef_name* **{ { deny [charging-action** *charging_action_name* **] } | { permit [nat-realm** *nat_realm_name* **| [trigger open-port {** *aux_port_number* **| range** *start_port_number* **to** *end_port_number* **} direction { both | reverse | same }]] } }**

no firewall priority *priority*

no

If previously configured, deletes the specified Stateful Firewall ruledef priority configuration from the current rulebase.

priority

Specifies the Stateful Firewall ruledef's priority in the current rulebase.
priority must be a unique value in the current rulebase, and must be an integer from 1 through 65535.

[dynamic-only | static-and-dynamic] firewall-ruledef *firewall_ruledef_name*

Specifies the Stateful Firewall ruledef to add to the rulebase. Optionally, the Stateful Firewall ruledef type can be specified.

- **dynamic-only**: Firewall Dynamic Ruledef—Predefined ruledef that can be enabled/disabled by the policy server, and is disabled by default.
- **static-and-dynamic**: Firewall Static and Dynamic Ruledef—Predefined ruledef that can be disabled/enabled by the policy server, and is enabled by default.
- *firewall_ruledef_name* must be the name of a Stateful Firewall ruledef, and must be an alphanumeric string of 1 through 63 characters.

deny [charging-action *charging_action_name* **]**

Denies packets if the rule is matched. An optional charging action can be specified. If a packet matches the deny rule, action is taken as configured in the charging action. For Stateful Firewall ruledefs, only the terminate-flow action is applicable, if configured in the specified charging action.
charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

permit [nat-realm *nat_realm_name* **| [bypass-nat] [trigger open-port {** *aux_port_number* **| range** *start_port_number* **to** *end_port_number* **}]]**

Permits packets.

- **nat-realm** *nat_realm_name*: Specifies the NAT realm to be used for performing NAT on subscriber packets matching the Stateful Firewall ruledef.

  If the NAT realm is not specified, then NAT will be bypassed. That is, NAT will not be applied on subscriber packets that are matching a Stateful Firewall ruledef with no NAT realm name configured.

  nat_realm_name must be the name of a NAT realm, and must be an alphanumeric string of 1 through 31 characters.

- **bypass-nat**: Specifies that packets bypass NAT.

  Important: If the **nat-realm** is not configured, NAT is performed if the **nat policy nat-required** CLI command is configured with the **default-nat-realm** option.

- **trigger open-port {** *aux_port_number* **| range** *start_port_number* **to** *end_port_number* **}**: Permits packets if the rule is matched, and allows the creation of data flows for Stateful Firewall. Optionally a port trigger can be specified to be used for this rule to limit the range of auxiliary data connections (a single or range of port numbers) for protocols having control and data connections (like FTP). The trigger port will be the destination port of an association which matches a rule.
  - *aux_port_number*: Specifies the number of auxiliary ports to open for traffic, and must be an integer from 1 through 65535.
  - **range** *start_port_number* **to** *end_port_number*: Specifies the range of ports to open for subscriber traffic.
    - *start_port_number* must be an integer from 1 through 65535. This is the start of the port range and must be less than *end_port_number*.
    - *end_port_number* must be an integer from 1 through 65535. This is the end of the port range and must be greater than *start_port_number*.

direction { both | reverse | same }

Specifies the direction from which the auxiliary connection is initiated. This direction can be same as the direction of control connection, or the reverse of the control connection direction, or in both directions.

- **both**: Provides the trigger to open port for traffic in either direction of the control connection.
- **reverse**: Provides the trigger to open port for traffic in the reverse direction of the control connection (from where the connection is initiated).
- **same**: Provides the trigger to open port for traffic in the same direction of the control connection (from where the connection is initiated).

Usage

Use this command to add Stateful Firewall ruledefs to the rulebase and configure the priority, type, and port triggers. Port trigger configuration is optional. Port trigger can be configured only if a rule action is permit. The rulebase specifies the Stateful Firewall rules to be applied on the calls. The ruledefs within a rulebase have priorities, based on which priority matching is done. Once a rule is matched and the rule action is

permit, if the trigger is configured, the appropriate check is made. The trigger port will be the destination port of an association which matches the rule.
Multiple triggers can be defined for the same port number to permit multiple auxiliary ports for subscriber traffic.
Once a rule is matched and if the rule action is deny, the action taken depends on what is configured in the specified charging action. If the flow exists, flow statistics are updated and action is taken as configured in the charging action:

- If the billing action is configured as EDR enabled, an EDR is generated.
- If the content ID is configured, UDR information is updated.
- If the flow action is configured as "terminate-flow", the flow is terminated instead of just discarding the packet.

If the billing action, content ID, and flow action are not configured, no action is taken on the dropped packets.

Important: For Stateful Firewall ruledefs, only the terminate-flow action is applicable if configured in the specified charging action.

For a packet dropped due to Stateful Firewall ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the **firewall priority** or the **firewall no-ruledef-matches** command respectively.
In StarOS 8.1, in the case of Policy-based Firewall, the charging action applied is the one configured in the **access-rule priority** or the **access-rule no-ruledef-matches** command respectively.
For action on packets dropped due to any error condition after data session is created, the charging action must be configured in the **flow any-error charging-action** command.
The GGSN can dynamically activate/deactivate dynamic Stateful Firewall ruledefs for a subscriber based on the rule name received from a policy server. At rule match, if a rule in the rulebase is a dynamic rule, and if the rule is enabled for the particular subscriber, rule matching is done for the rule. If the rule is disabled for the particular subscriber, rule matching is not done for the rule.

Example

The following command assigns a priority of *10* to the Stateful Firewall ruledef *fw_rule1*, adds it to the rulebase, and permits port trigger to be used for the rule to open ports in the range of *100* to *200* in either direction of the control connection:

```
firewall priority 10 firewall-ruledef fw_rule1 permit trigger open-port
range 100 to 200 direction both
```

The following command configures the Stateful Firewall ruledef *fw_rule2* as a dynamic ruledef:

```
firewall priority 7 dynamic-only firewall-ruledef fw_rule2 deny
```

firewall tcp-first-packet-non-syn

This command allows you to configure the action to take on TCP flows starting with a non-syn packet.

Important: In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
firewall tcp-first-packet-non-syn { drop | reset }

default firewall tcp-first-packet-non-syn
```

default

Configures this command with its default setting.
Default: **drop**

drop

Specifies to drop the packet or session.

reset

Specifies to send reset.

Usage

Use this command to configure action to take on TCP flow starting with a non-syn packet.

Example

The following command configures action to take on TCP flow starting with a non-syn packet to drop:

```
firewall tcp-first-packet-non-syn drop
```

firewall tcp-idle-timeout-action

This command allows you to configure the Stateful Firewall action to be taken on TCP idle timeout expiry.

Important: In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
firewall tcp-idle-timeout-action { drop | reset }

default firewall tcp-idle-timeout-action
```

default

Configures this command with its default setting.
Default: **reset**

drop

Specifies to drop the packet or session on TCP timeout expiry.

reset

Specifies to send reset on TCP timeout expiry.

Usage

Use this command to configure action to take on TCP idle timeout expiry.

Example

The following command configures action to take on TCP idle timeout expiry to drop:

```
firewall tcp-idle-timeout-action drop
```

firewall tcp-reset-message-threshold

This command allows you to configure a threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. After this threshold is reached, further downlink traffic to the subscriber on the unwanted flow is blocked.

Important: This command is only available in StarOS 8.3 and later releases. In StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall tcp-reset-message-threshold *messages* **then-block-server**

{ default | no } firewall tcp-reset-message-threshold

default

Configures this command with its default setting.
Default: **no firewall tcp-reset-message-threshold**

no

If previously configured, deletes the firewall tcp-reset-message-threshold configuration from the current rulebase.

messages

Specifies the threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. *messages* must be an integer from 1 through 100.

Usage

Use this command to configure a threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. After the threshold is reached, assuming the server is not reacting properly to the reset messages further downlink traffic to the subscriber on the unwanted flow is blocked. This configuration enables QCHAT noise suppression for TCP.

Example

The following command sets the threshold on the number of TCP reset messages to *10*:

```
firewall tcp-reset-message-threshold 10 then-block-server
```

firewall tcp-syn-flood-intercept

This command allows you to configure the TCP intercept parameters to prevent TCP SYN flooding attacks by intercepting and validating TCP connection requests for DoS protection mechanism configured with the **dos-protection** command.

Important: In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall tcp-syn-flood-intercept { mode { none | watch [aggressive] } | watch-timeout *intercept_watch_timeout* **}**

default firewall tcp-syn-flood-intercept { mode | watch-timeout }

default

Sets the default values of TCP intercept parameters for SYN Flood DoS protection.

mode { none | watch [aggressive] }

Specifies the TCP SYN flood intercept mode:

- **none**: Disables TCP SYN flood intercept feature.
- **watch**: Configures TCP SYN flood intercept feature in watch mode. Stateful Firewall passively watches to see if TCP connections become established within a configurable interval. If connections are not established within the timeout period, Stateful Firewall clears the half-open connections by sending RST to TCP client and server. The default watch-timeout for connection establishment is 30 seconds.
- **aggressive**: Configures TCP SYN flood Intercept or Watch feature for aggressive behavior. Each new connection request causes the oldest incomplete connection to be deleted. When operating in watch mode, the watch timeout is reduced by half. If the watch-timeout is 30 seconds, under aggressive conditions it becomes 15 seconds. When operating in intercept mode, the retransmit timeout is reduced by half (i.e. if the timeout is 60 seconds, it is reduced to 30 seconds). Thus the amount of time waiting for connections to be established is reduced by half (i.e. it is reduced to 150 seconds from 300 seconds under aggressive conditions).

Default: **none**

watch-timeout *intercept_watch_timeout*

Specifies the TCP intercept watch timeout, in seconds.
intercept_watch_timeout must be an integer from 5 through 30.
Default: 30

Usage

This TCP intercept functionality provides protection against TCP SYN Flooding attacks.
The system captures TCP SYN requests and responds with TCP SYN-ACKs. If a connection initiator completes the handshake with a TCP ACK, the TCP connection request is considered as valid by system and system forwards the initial TCP SYN to the valid target which triggers the target to send a TCP SYN-ACK. Now system intercepts with TCP SYN-ACK and sends the TCP ACK to complete the TCP handshake. Any TCP packet received before the handshake completion will be discarded.

Example

The following command sets the TCP intercept watch timeout setting to *5* seconds:

```
firewall tcp-syn-flood-intercept watch-timeout 5
```

flow any-error

This command allows you to specify the charging action to be used for packets dropped by Stateful Firewall due to any error conditions.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

flow any-error charging-action *charging_action_name*

default flow any-error

default

Configures the default action for packets dropped by Stateful Firewall due to any errors.
Default: Update the flow statistics if flow is available

charging_action_name

Specifies the charging action based on which accounting action is taken on packets dropped by Stateful Firewall due to any errors.
charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

Important: The charging action specified here should preferably not be used for action on packets dropped due to Stateful Firewall ruledef match or no-match (in the **firewall priority** and **firewall no-ruledef-matches** commands) and the content ID within the charging action must be unique so that dropped counts will not interfere with other content IDs.

Usage

Use this command to configure the charging action for packets dropped by Stateful Firewall due to any error conditions, such as, a packet being inappropriate based on the state of the protocol of the packet's session, or DoS protection causing the packet to be discarded, and so on.
For a packet dropped due to Stateful Firewall ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the **firewall priority** or the **firewall no-ruledef-matches** command respectively.
In StarOS 8.1, in the case of Policy-based Firewall, the charging action applied is the one configured in the **access-rule priority** or the **access-rule no-ruledef-matches** command respectively.
For a packet dropped due to any error condition after data session is created, the charging action used is the one configured in the **flow any-error charging-action** command.
If the charging action applied on a packet is the one specified in the **flow any-error charging-action** command, flow statistics are updated and action is taken as configured in the charging action:

- If the billing action is configured as EDR enabled, an Event Data Record (EDR) is generated.
- If the content ID is configured, Usage Data Record (UDR) information is updated.

- If the flow action is configured as “terminate-flow”, the flow is terminated instead of just discarding the packet.

If the billing action, content ID, and flow action are not configured, no action is taken on the dropped packets.

Example

The following command specifies the charging action *test2* for accounting action on packets dropped/discarded by Stateful Firewall due to any error:

```
flow any-error charging-action test2
```

flow control-handshaking

This command allows you to specify how to charge for the control traffic associated with an application.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
flow control-handshaking { charge-to-application { [ all-packets ] [ initial-packets ] [
mid-session-packets ] [ tear-down-packets ] } | charge-separate-from-application }

default flow control-handshaking

no flow control-handshaking [ charge-to-application ]
```

`default flow control-handshaking`

Configures this command with its default setting.
Default: Same as **`no flow control-handshaking`**

`no flow control-handshaking [ charge-to-application ]`

If previously configured, deletes the flow control-handshaking configuration from the current rulebase. The control packets will use whatever content-id is determined by the normal use of the **`action`** commands.
In this command, the optional keyword **`charge-to-application`** is deprecated and has no effect.

`charge-to-application { [ all-packets ] [ initial-packets ] [ mid-session-packets ] [ tear-down-packets ] }`

Configures the charging action to include the flow control packets either during initial handshaking only or specified control packets during session for charging.

- **`all-packets`**: Specifies that the initial setup packets will wait until the application has been determined before assigning the content-id, and all mid-session ACK packets as well as the final tear-down packets will use that content-id.
- **`initial-packets`**: Specifies that only the initial setup packets will wait for content-id assignment.
- **`mid-session-packets`**: Specifies that the ACK packets after the initial setup will use the application's or content-id assignment.
- **`tear-down-packets`**: Specifies that the final tear-down packets (TCP or WAP) will use the application's or content-id assignment.

`charge-separate-from-application`

Configures the charging action to separate the charging of the initial control packets or all subsequent control packets from regular charging.

Usage

Use this command to configure how to charge for the control traffic associated with an application ruledef. Applications like HTTP use TCP to set up and tear down connections before the HTTP application starts.

This command controls whether the packets that set up and tear down the connections should use the same content ID as the application's flow.
In normal mode 3-way handshake TCP packets (SYN, SYN-ACK, and ACK) and closing or intermittent packets (FIN, RST, etc.) directed and charged based on configured matched rules. This command makes the system to wait for the start and stop of layer 7 packet flow and content ID and charge the initial, intermittent, and closing TCP packets as configured to the same matching rules and content ID as of the flow.
This command also affects applications that do not use TCP but use other methods for control packets, for example WAP, where WTP/UDP may be used to set up and tear down connection-oriented WSP.

Example

Following command enables the charging for initial TCP handshaking control packets and wait for content-id of data traffic flow:

```
flow control-handshaking charge-to-application initial-packets
```

The following command enables charging all mid-session ACKs as well as tear-down packets to application:

```
flow control-handshaking charge-to-application mid-session-packets tear-down-packets
```

flow end-condition

This command allows you to configure the end condition of the session flows related to a user session and triggers EDR generation.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

In 12.1 and earlier releases:

flow end-condition { { content-filtering | normal-end-signaling | timeout + } | { { hagr | handoff | session-end } [flow-overflow] + } [url-blacklisting] } edr *edr_format_name*

no flow end-condition

In 12.2 and later releases:

flow end-condition { content-filtering | hagr | handoff | normal-end-signaling | session-end | url-blacklisting | timeout } [flow-overflow] + { charging-edr *charging_edr_format_name* **| reporting-edr** *reporting_edr_format_name* **}**

no flow end-condition

no

If previously configured, deletes the flow end-condition configuration from the current rulebase.

content-filtering

Creates an EDR with the specified EDR format whenever a flow ends due to Category-based Content Filtering in-line service action. Possible actions include redirect-url, terminate-flow, content-insert.

hagr

Creates an EDR with the specified EDR format whenever a flow is terminated due to Inter-chassis Session Recovery action.

handoff

Creates an EDR with the specified EDR format whenever a flow ends due to hand-off. Whenever a handoff occurs, ACS closes the EDRs for all current flows using the specified EDR format, and begins new statistics collection for the flows for the EDRs that will be generated when the flows actually end.

normal-end-signaling

Creates an EDR with the specified EDR format whenever flow end is signaled normally, for example like detecting FIN and ACK for a TCP flow, or a WSP-DISCONNECT terminating a connection-oriented WSP flow over UDP) and create an EDR for the flow using the specified EDR format.

session-end

Creates an EDR with the specified EDR format whenever a subscriber session ends. By this option ACS creates an EDR with the specified format name for every flow that has had any activity since last EDR was created for the flow on session end.

url-blacklisting

Creates an EDR with the specified EDR format whenever flow ends due to URL Blacklisting action.

timeout

Creates an EDR with the specified EDR format whenever a flow ends due to a timeout condition.

flow-overflow

Important: This keyword is only available in StarOS 8.3 and later releases. And, is only applicable when used with the **hagr**, **handoff**, and **session-end** keywords.

Creates an EDR with the specified EDR format whenever there is a flow-overflow condition. If any of the specified end-conditions that affect subscriber information stored at ACS (such as call line) is configured, the "flow-overflow" EDR is generated.

+

Indicates that more than one of the keywords can be entered within a single command.

edr *edr_format_name*

Important: This option is available only in the 12.1 and earlier releases. In 12.2 and later releases, this option is deprecated and is replaced by the **charging-edr** option.

Specifies the EDR format to record EDR for specified flow end condition.
edr_format_name must be the name of an EDR format, and must be a unique alphanumeric string of 1 through 63 characters.

charging-edr *charging_edr_format_name*

Important: This option is available only in 12.2 and later releases.

Specifies the charging EDR format.
charging_edr_format_name must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

reporting-edr *reporting_edr_format_name*

Important: This option is available only in 12.2 and later releases.

Specifies the reporting EDR format.

reporting_edr_format_name must be the name of a reporting EDR format, and must be a unique alphanumeric string of 1 through 63 characters.

Usage

Use this command to enable or disable the capturing of EDRs based on flow end condition.

Example

In 12.1 and earlier releases, the following command configures the flow end condition as "handoff" and creates a charging EDR with format named *EDR_format1*:

```
flow end-condition handoff edr-format EDR_format1
```

In 12.2 and later releases, the following command configures the flow end condition as handoff and creates a charging EDR with format named *EDR_format1*:

```
flow end-condition handoff charging-edr EDR_format1
```

flow limit-across-applications

This command allows you to limit the total number of simultaneous flows per Subscriber/APN sent to a rulebase regardless of the flow type, or limit flows based on the protocol type under the Session Control feature.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
flow limit-across-applications { limit | non-tcp limit | tcp limit }

no flow limit-across-applications [ non-tcp | tcp ]
```

no

If previously configured, deletes the flow limit-across-applications configuration from the current rulebase.

flow limit-across-applications *limit*

Specifies the maximum number of flows across all applications for the rulebase.
limit must be an integer from 1 through 4000000000.
Default: No limits

non-tcp *limit*

Specifies the maximum limit of non-TCP type flows.
limit must be an integer from 1 through 4000000000.
Default: No limits

tcp *limit*

Specifies the maximum limit of TCP flows.
limit must be an integer from 1 through 4000000000.
Default: No limits

Usage

Use this command to limit the total number of flows allowed for a rulebase regardless of flow type, or limit flows based on the protocol—non-TCP (connection-less) or TCP (connection-oriented).
If a subscriber attempts to exceed these limits system discards the packets of new flow. This limit processing of this command has following aspects for UDP, TCP, ICMP and some of the exempted flows:

- UDP/ICMP: System waits for the flow timeout before updating the counter and removing it from the count of number of flows.
- TCP: After a TCP flow ends, system waits for a short period of time to accommodate the retransmission of any missed packet from one end. TCP flows those are ended, but are still in wait period for timeout are exempted for this limit processing.
- Exempted flows: System exempts all the other flows specified with the **flow limit-for-flow-type** command in the ACS Charging Action Configuration Mode set to **no**.

Example

The following command defines the maximum number of *200000* flows for the rulebase:

```
flow limit-across-applications 200000
```

fw-and-nat default-policy

This command allows you to configure the default Firewall-and-NAT policy for the current rulebase. This command must be used to configure the Policy-based Firewall-and-NAT feature.

Important: This command is only available in StarOS 8.1 and StarOS 9.0 and later releases.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

fw-and-nat default-policy *fw_nat_policy_name*

no fw-and-nat default-policy

no

If previously configured, deletes the Firewall-and-NAT default policy configuration from the current rulebase.

fw_nat_policy_name

Specifies the default Firewall-and-NAT policy for the current rulebase.
fw_nat_policy_name must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the default Firewall-and-NAT policy for a rulebase.
For subscribers using the current rulebase, the default Firewall-and-NAT policy will be used if in the APN/subscriber profile the **default fw-and-nat policy** command is configured, and a policy to use is not received from the AAA/OCS.
For more information, see the *Personal Stateful Firewall Administration Guide*.

Example

The following command configures a Firewall-and-NAT policy named *standard* to the rulebase:

```
fw-and-nat default-policy standard
```

ip reassembly-timeout

This command allows you to configure how long to hold onto IP fragments for reassembly, while waiting for the complete packet to arrive.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

ip reassembly-timeout *timeout_duration*

default ip reassembly-timeout

default

Configures the default setting for this command.
Default: 5000 milliseconds

timeout_duration

Specifies the timeout duration, in milliseconds, to hold fragmented packets before reassembly.
timeout_duration must be an integer from 100 through 30000.

Usage

Use this command to configure duration for timeout timer to hold IP fragmented packets before reassembly is needed.
IP fragmented packet are retained, until either all fragmented packets have been received or the configured timeout has expired for the oldest fragment. If all fragments have been received, a temporary complete packet is reconstructed for analysis. Then all fragments are forwarded in order from first to last. If all fragments are not received, the fragments will be forwarded without being passed through the protocol analyzers, except for the IP analyzer.

Example

The following command sets the timeout timer to *15000* milliseconds:

```
ip reassembly-timeout 15000
```

ip reset-tos

This command allows you to reset the IP Type of Service (ToS) value of incoming packets to zero, before proceeding with the rest of ACS processing.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] ip reset-tos
```

default

Configures this command with its default setting.
Default: Disabled

no

If previously configured, deletes the IP reset-tos configuration from the current rulebase.

Usage

Use this command to reset the ToS field of any packet after it reaches ACS, or to broaden the range of values that are used in the ToS field in the IP header of any packet.

nat binding-record

This command allows you to configure NAT Binding Record (NBR) generation.

Important: This command is only available in StarOS 8.3. In StarOS 9.0 and later releases this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

nat binding-record edr-format *edr_format_name* **[port-chunk-allocation] [port-chunk-release] +**

{ default | no } nat binding-record

default

Configures this command with its default setting.
Default: **port-chunk-release**

no

If previously configured, deletes the configuration from the current rulebase.

edr-format *edr_format_name*

Specifies the EDR format.
edr_format_name must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.

port-chunk-allocation

Specifies generating NBR when a port chunk is allocated.

port-chunk-release

Specifies generating NBR when a port chunk is released.

+

Indicates that more than one of the previous keywords can be entered within a single command.

Usage

Use this command to configure NBR generation.

Example

The following command configures an EDR format named *test123* and specifies generating NBR when a port chunk is allocated, and when a port chunk is released:

```
nat binding-record edr-format test123 port-chunk-allocation port-chunk-
release
```

nat policy

This command allows you to enable/disable Network Address Translation (NAT) processing for all subscribers using the current rulebase.

Important: In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Important: Before enabling NAT processing for a subscriber, Stateful Firewall must be enabled for the subscriber. See the firewall policy CLI command.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

nat policy nat-required [default-nat-realm *nat_realm_name* **]**

{ default | no } nat policy

default

Configures this command with its default setting.
Default: NAT processing is disabled for all subscribers using the current rulebase.

no

If previously enabled, disables NAT processing for all subscribers using the current rulebase.

nat policy nat-required

Enables NAT processing for all subscribers using the current rulebase.

default-nat-realm *nat_realm_name*

Important: This keyword is only available in StarOS 8.3 and later releases.

Specifies the default NAT realm to be used if one is not already configured.
nat_realm_name must be the name of a NAT realm, and must be an alphanumeric string of 1 through 31 characters.

Important: Including the default NAT realm, a maximum of three NAT realms are supported.

Usage

Use this command to enable/disable NAT processing for all subscribers using the current rulebase.

After NAT is enabled for a subscriber, the NAT IP address to be used is chosen from the NAT realms defined in the rule priority lines within the rulebase. See the firewall priority CLI command.
NAT enable/disable status in the rulebase can be changed any time, however the changed NAT status will not be applied for active calls using the rulebase. The new NAT status is only applied to new calls.

Example

The following command enables NAT processing:

```
nat policy nat-required
```

The following command disables NAT processing:

```
no nat policy
```

nat suppress-aaa-update call-termination

This command allows you to suppress sending NAT Bind Updates (NBU) to the AAA server when a call gets terminated.

Important: This command is customer-specific. For more information please contact your Cisco account representative. In release 9.0, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

```
nat suppress-aaa-update call-termination

default nat suppress-aaa-update
```

default

Configures this command with its default setting.
Default: Disabled. No suppression of AAA updates.

Usage

Use this command to suppress the sending of NAT Bind Updates (NBU) to the AAA server when the call gets terminated, as these NBUs would be cleared at the AAA after receiving the accounting-stop. This enables to minimize the number of messages between the chassis and AAA server. When not configured, NBUs are sent to the AAA server whenever a port chunk is allocated, de-allocated, or the call is cleared (PPP disconnect).

Example

The following command suppresses the sending of NBU to the AAA server when PPP disconnect happens:

```
nat suppress-aaa-update call-termination
```

p2p dynamic-flow-detection

This command allows you to enable/disable the P2P analyzer to detect peer-to-peer (P2P) applications.

Product

ADC

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] p2p dynamic-flow-detection
```

default

Configures this command with its default setting.
Default: Disabled

no

If previously enabled, disables P2P dynamic flow detection in the current rulebase.

p2p dynamic-flow-detection

Enables dynamic P2P flow detection.

Usage

Use this command to enable dynamic-flow detection. This allows the P2P analyzer to detect the P2P applications configured for the ACS.

post-processing dynamic

This command allows you to specify ruledefs/group-of-ruledefs as dynamic post-processing ruledefs/group-of-ruledefs. This allows the system to differentiate normal post-processing rules from preconfigured ones. By default, this configuration is disabled.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
post-processing dynamic { group-of-ruledefs ruledefs_group_name | ruledef ruledef_name }
charging-action charging_action_name [ description description ]

no post-processing dynamic { group-of-ruledefs ruledefs_group_name | ruledef ruledef_name
}
```

no

If previously configured, deletes the specified configuration from the current rulebase.

group-of-ruledefs *ruledefs_group_name*

Adds the specified group-of-ruledefs to the current rulebase.
ruledefs_group_name must be the name of a group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.

ruledef *ruledef_name*

Adds the specified ruledef to the current rulebase.
ruledef_name must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

charging-action *charging_action_name*

Specifies the charging action.
charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

description *description*

Specifies an optional description for this configuration.
description must be an alphanumeric string of 1 through 31 characters.

Usage

Use this command to configure specific ruledefs/group-of-ruledefs as dynamic post-processing ruledefs/group-of-ruledefs. This allows the system to differentiate normal post-processing rules from the preconfigured ones. This makes possible enabling/disabling ruledefs/groups-of-ruledefs entry from an external server.

Example

The following command specifies the ruledef named *test_rule* as a dynamic post-processing ruledef configured with the charging action *ca13* and a description of *testing*:

```
post-processing dynamic ruledef test_rule charging-action ca13
description testing
```

post-processing policy

This command allows you to specify the post-processing policy to be applied on Limit-Reached packets.

Product

GGSN, P-GW, PDSN

Privilege

Security Administrator, Administrator

Syntax

```
post-processing policy { always | not-for-dynamic-discard }

default post-processing policy
```

default

Configures this command with its default setting.
Default: **not-for-dynamic-discard**

always

Specifies to apply post-processing even if the Credit Control Application (CCA) decides to discard packets due to limit-reached condition. If there are post-processing priority-based rules, CCA will check for any redirection rules. Otherwise, by default, CCA will discard the packets. No other post-processing actions like forward, next-hop, or xheader-insertion will be applied on the limit-reached packets.

not-for-dynamic-discard

Specifies to apply post-processing only if CCA decides not to discard packet. Will directly discard the limit-reached context and will not apply post-processing priority based rules.

Usage

This command allows to enable post-processing priority based rules for content in blacklisted state. Whenever RADIUS/Diameter prepay server blacklists content the packets are generally discarded. To enable redirection of such content, post-processing should be enabled on the blacklisted content. With this command, RADIUS/Diameter Credit-Control application will decide whether to allow post-processing to be enabled or not for the blacklisted content.
The following is a sample configuration:

```
configure
 active-charging service service1
 ruledef http_low
 http any-match = TRUE
 cca quota-state = limit-reached
 rule-application post-processing
 #exit
```

```
ruledef httpany
http any-match = TRUE
#exit
charging-action standard1
content-id 1
cca charging credit
#exit
charging-action redirect
flow action redirect-url http://aoc.com
#exit
rulebase base1
action priority 30 ruledef httpany charging-action standard1
post-processing policy always
post-processing priority 1 ruledef http_low charging-action redirect
#exit
end
```

Example

The following command will enable post processing on Limit-Reached packets:

```
post-processing policy always
```

post-processing priority

This command allows you to configure the post-processing priority and action to be taken on specific ruledef in the current rulebase.

Important: This command is only available in StarOS 8.3 and later releases.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

post-processing priority *priority* **{ group-of-ruledefs** *ruledefs_group_name* **| ruledef** *ruledef_name* **} charging-action** *charging_action_name* **[description** *description* **]**

no post-processing priority *priority*

no

If previously configured, deletes the specified post-processing priority configuration from the current rulebase.

priority *priority*

Specifies priority for the ruledef/group-of-ruledefs in the current rulebase.
priority must be a unique value in the current rulebase, and must be an integer from 1 through 65535.

group-of-ruledefs *ruledefs_group_name*

Specifies the group-of-ruledefs.
ruledefs_group_name must be the name of a group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.

Important: The group-of-ruledefs specified must be configured for post-processing. See the **group-of-ruledefs-application** command in the ACS Group-of-Ruledefs Configuration mode.

ruledef *ruledef_name*

Specifies the ruledef.
ruledef_name must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

Important: The ruledef specified must be configured for post-processing. See the **rule-application** command in the *ACS Ruledef Configuration Mode Commands* chapter.

charging-action *charging_action_name*

Specifies the charging action.

charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

description *description*

Specifies an optional description for this configuration.
description must be an alphanumeric string of 1 through 31 characters.

Usage

Use this command to configure the post-processing priority and action to be taken on a ruledef in the rulebase.

Example

The following command configures the ruledef named *test_ruledef* with a priority of *10*, and the charging action named *test_ca* for post processing:

```
post-processing priority 10 ruledef test_ruledef charging-action test_ca
```

qos-renegotiate timeout

This command allows you to configure the timeout setting for the Quality of Service (QoS) Renegotiation feature.

Important: This command is license dependent. For more information contact your Cisco account representative.

Product

All

Privilege

Security Administrator, Administrator

Syntax

qos-renegotiate timeout *timeout*

no qos-renegotiate timeout

no

If previously configured, deletes the qos-renegotiate timeout configuration from the current rulebase.

timeout

Specifies the timeout period for the QoS Renegotiation feature in the current rulebase.
timeout is the timeout period in seconds, and must be an integer from 0 through 4294967295. If set to 0, timeout is disabled.

Usage

Use this command to configure timeout setting for the QoS Renegotiation feature.

Example

The following command sets the QoS renegotiate timeout period to 1000 seconds:

```
qos-renegotiate timeout 1000
```

radius threshold

This command allows you to configure the interval and volume thresholds to generate interim RADIUS Charging Data Records (CDRs) and write them to CDR file for ACS postpaid billing.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
radius threshold { interval interval | volume total volume }

{ default | no } radius threshold { interval | volume total }
```

no

If previously configured, deletes the RADIUS threshold configuration from the current rulebase.

default

Configures this command with the default settings.
Default: Disabled

interval *interval*

Specifies the time interval, in seconds, for generating RADIUS interim accounting requests.
interval must be an integer from 60 through 40000000.
Default: Disabled

volume total *volume*

Specifies the limit for the total number of octets (uplink+downlink) after which a stop-start pair will be sent to RADIUS.
volume must be an integer from 100000 through 4000000000.
Default: Disabled

Usage

Use this command to specify a time interval threshold to generate interim RADIUS CDRs and write it to RADIUS CDR file for postpaid billing.

Example

The following command configures a time threshold interval of *600* seconds for RADIUS CDRs:

```
radius threshold interval 600
```

route priority

This command allows you to configure the routing of packets to protocol analyzers.

Product

All

Privilege

Security Administrator, Administrator

Syntax

route priority *route_priority* **ruledef** *ruledef_name* **analyzer { dns | file-transfer | ftp-control | ftp-data | h323 | http | imap | mms | p2p | pop3 | pptp | rtcp | rtp | rtsp | sdp | secure-http | sip [advanced | basic-and-advanced] | smtp | tftp | wsp-connection-less | wsp-connection-oriented } [description** *description* **]**

no route priority *route_priority*

---

no

If previously configured, deletes the specified route priority configuration from the current rulebase.

---

route priority *route_priority*

Specifies the route priority for the specified ruledef in the current rulebase.
route_priority must be an integer from 1 through 65535.
Lower numbered priorities are examined first. Up to 1024 instances can be configured across all rulebases.

---

ruledef *ruledef_name*

Specifies the ruledef to evaluate packets to determine analyzer.
ruledef_name specifies the name of the ruledef configured for the route application using the **rule-application** command in the ACS Ruledef Configuration Mode.
ruledef_name must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

---

analyzer

Specifies the analyzer for the ruledef, and must be one of the following:

- **dns**: Route to DNS protocol analyzer.
- **file-transfer**: Route to file analyzer.
- **ftp-control**: Route to FTP control protocol analyzer.
- **ftp-data**: Route to FTP data protocol analyzer.
- **h323**: Route to H323 protocol analyzer.
- **http**: Route to HTTP protocol analyzer.
- **imap**: Route to IMAP protocol analyzer.
- **mms**: Route to MMS protocol analyzer.
- **p2p**: Route to the P2P protocol analyzer.
- **pop3**: Route to POP3 protocol analyzer.

- **pptp**: Route to PPTP protocol analyzer.
- **rtcp**: Route to RTCP protocol analyzer.
- **rtp**: Route to RTP protocol analyzer.
- **rtsp**: Route to RTSP protocol analyzer.
- **sdp**: Route to SDP protocol analyzer.
- **secure-http**: Route to secure HTTP protocol analyzer.
- **sip [advanced | basic-and-advanced]**: Route to SIP protocol analyzer.
  - **advanced**: For SIP calls to work with NAT/Stateful Firewall, a SIP Application-Level Gateway (ALG) is required to do payload translation of SIP packets and pin-hole (dynamic flow) creation for media packets. A SIP routing rule must to be configured for routing the packets to the SIP ALG for processing. If the keyword **advanced** is configured, the packets matching the routing rule will be routed to SIP ALG for processing and not to ACS SIP analyzer. If not configured, then packets will not be routed to SIP ALG and will be routed to ACS SIP analyzer for processing.

    Also, see **firewall nat-alg** CLI command in the ACS Configuration Mode.
  - **basic-and-advanced**: For SIP ALG to co-exist with SIP Analyzer, the packets are routed through ACS SIP Analyzer and SIP ALG. The SIP packets can pass through ACS functionality (by ACS SIP Analyzer processing) and at the same time payload translation/pinhole-creation can happen successfully (by SIP ALG processing). If **basic-and-advanced** is configured, then the packets matching the routing rule will be routed through the SIP Analyzer and then through SIP ALG for processing.
- **tftp**: Route to TFTP protocol analyzer.
- **smtp**: Route to SMTP protocol analyzer.
- **wsp-connection-less**: Route to WSP connection-less protocol analyzer.
- **wsp-connection-oriented**: Route to WSP connection-oriented protocol analyzer.

Important: To route packets to the P2P analyzer, the ruledef should have rules to match all IP packets. Otherwise, the analyzer may not detect all P2P traffic.

Important: Use the **show active-charging analyzer statistics** command in the Exec Mode to see the list of supported analyzers.

description *description*

Enables to add a description to the rule and action for later reference in saved configuration file. *description* must be an alphanumeric string of 1 through 63 characters.

Usage

Instances of this CLI command control which packets are routed to which protocol analyzers. Packets sent to ACS are always passed through the IP protocol analyzer. This CLI command controls which higher layer analyzers are also invoked.

Analyzer	Common ways to route to the analyzer
ip	All IPv4 packets are automatically routed here.

Analyzer	Common ways to route to the analyzer
icmp	All IPv4 packets with IP protocol = ICMP (1) are automatically routed here.
tcp	All IPv4 packets with IP protocol = TCP (6) are automatically routed here.
udp	All IPv4 packets with IP protocol = UDP (17) are automatically routed here.
dns	UDP destination port or source port is DNS (53).
http	TCP destination port or source port is HTTP (80).
secure-http	TCP destination port or source port is HTTPS (443). Note that HTTP may use the CONNECT method (see RFC 2817), in which case, the subscriber will be upgraded with transport layer security, but the traffic to/from the chassis will still be HTTP and be passed through the http rather than the secure-http analyzer (assuming that routing to the http analyzer has been configured).
wsp	UDP destination port or source port is connection-less WSP (9200) or connection-oriented WSP (9201).
wtp	Packets are automatically routed here, if you specified "wsp-connection-oriented" as described above.
wap2	TCP destination port or source port of the carrier-specific port number for WAP-2 (e.g. one carrier uses 8799); or, send all HTTP traffic to the **wap2** analyzer if the carrier does not use a special port number.
ftp	TCP destination port or source port is FTP control (21) or FTP data (20); or, ftp analyzer (for FTP control packets) dynamically detected an FTP data flow over TCP (tcp dynamic-flow = ftp-data).
file-transfer	FTP and the command name is **retr** or **stor**; or, HTTP and the request method is **get** or **post**.
mms	WSP content type is application/vnd.wap.**mms**-message; or, WSP uri contains "**mms**"; or, HTTP content type is application/vnd.wap.mms-message; or, HTTP uri contains "**mms**".
sip	UDP destination port or source port is SIP (5060).
sdp	RTSP or SIP content type is application/sdp
smtp	TCP destination port or source port is SMTP (25).
imap	TCP destination port or source port is IMAP (143).
pop3	TCP destination port or source port is POP3 (110).
rtp and **rtcp**	RTSP has embedded RTP/RTCP payloads (you need to enable RTP dynamic flow detection to catch those flows); or, RTSP or SDP (for SDP within SIP) creates an RTP/RTCP flow over UDP (in addition to enabling the aforementioned dynamic flow detection, you must make sure that UDP packets are routed to the UDP analyzer) or, RTP/RTCP uses predefined UDP port numbers (e.g. default UDP port numbers of 5004/5005).
rtsp	TCP destination port or source port is RTSP (554).
p2p	Use the **p2p dynamic-flow-detection** CLI command to enable detection of the different P2P applications specified by the **p2p application** CLI command; that will cause every TCP or UDP packet to be automatically routed here

Example

The following command assigns a route and rule action with the route priority of 23, a ruledef named *test*, and an analyzer *test_analyzer* with description as *route_test1* to the current rulebase:

```
route priority 23 ruledef test analyzer test_analyzer description
route_test1
```

rtp dynamic-flow-detection

This command allows you to enable/disable the Real Time Streaming Protocol (RTSP) and Session Description Protocol (SDP) analyzers to detect the start/stop of RTP and RTCP flows.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ default | no ] rtp dynamic-flow-detection`

`default`

Configures this command with its default setting.
Default: Disabled; same as **`no rtp dynamic-flow-detection`**.

`no`

If previously configured, deletes this configuration from the current rulebase.

Usage

Use this command to enable the RTSP and SDP analyzer to detect the start/stop of RTP and RTCP flows. This command is used in conjunction with the **`route priority`** command.

Example

The following command enables RTP dynamic flow detection:

```
rtp dynamic-flow-detection
```

ruledef-parsing

This command allows you to configure whether to consider or ignore the port number embedded in the application header (for example, the ":80" in www.star.com:80) when comparing the ruledef expressions to the packet contents.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ruledef-parsing ignore-port-numbers-embedded-in-application-headers analyzers { http rtsp sip wsp }

default ruledef-parsing
```

no

If previously configured, deletes the ruledef-parsing configuration from the current rulebase.

default

Configures this command with its default setting.
Default: Same as **no ruledef-parsing ignore-port-numbers-embedded-in-application-headers analyzers { http rstp sip wsp }**— not ignoring port numbers that are embedded in application headers.

ignore-port-numbers-embedded-in-application-headers analyzers { http rtsp sip wsp }

Ignore the port numbers present in application header.
Specifies analyzers for which the port number must be ignored.

Usage

Use this command to make the HTTP, RTSP, SIP, and WSP analyzer ignore port numbers embedded in application headers.

Example

The following command makes the HTTP analyzer in the current rulebase ignore port numbers embedded in application headers:

```
ruledef-parsing ignore-port-numbers-embedded-in-application-headers analyzers http
```

tcp 2msl-timeout

This command allows you to configure how long to retain the TCP flow after the FIN has been acknowledged.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

tcp 2msl-timeout *2msl_timeout*

{ default | no } tcp 2msl-timeout

default

Configures this command with its default setting.
Default: 2 seconds

no

Disables the timeout and sets the system to delete the flow immediately upon seeing the FIN acknowledged.

tcp 2msl-timeout *2msl_timeout*

Specifies the duration to keep the TCP flow.
2msl_timeout specifies the timeout duration, in seconds, and must be an integer from 1 through 20.

Usage

Use this command to configures how long to retain the TCP flow after the FIN has been acknowledged. Acknowledgment to the FIN is not guaranteed to be received by the destination, then the FIN could be resent and re-acknowledged. In this scenario, it is desirable to still have the flow, so that the re-sends do not create a new flow.

Example

The following command sets the timeout to 4 seconds:

```
tcp 2msl-timeout 4
```

tcp check-window-size

This command allows you to enable/disable TCP window-size checking.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] tcp check-window-size
```

default

Configures this command with its default setting.
Default: Enabled (packets after the erroneous packet (with size greater than the receiver's window size) will hit tcp-error ruledef).

no

Disables the window-size check and continues with normal L7 parsing.

tcp check-window-size

Enables the window-size check and continues with normal L7 parsing.

Usage

Use this command to enable/disable TCP window-size check for packets out of TCP window.

Example

The following command enables TCP window-size check:

```
tcp check-window-size
```

tcp mss

This command allows you to configure the TCP Maximum Segment Size (MSS) in TCP SYN packets.

Important: This command is only available in StarOS 8.1 and later releases.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

tcp mss *tcp_mss* **{ add-if-not-present | limit-if-present } +**

{ default | no } tcp mss

default

Configures this command with its default setting.
Default: Disabled

no

If previously configured, deletes the TCP MSS configuration from the current rulebase.

tcp mss *tcp_mss*

Specifies the TCP MSS.
tcp_mss must be an integer from 496 through 65535.

add-if-not-present

Specifies to add the TCP MSS if not present in the packet.

limit-if-present

Specifies to limit the TCP MSS if present in the packet.

Usage

Using this command, TCP MSS can be limited if already present in the TCP SYN packets. If there are no errors detected in IP header/TCP mandatory header and there are no memory allocation failures, TCP optional header is parsed. If TCP MSS is present in the optional header and its value is greater than the configured MSS value, the value present in the TCP packet is replaced with the configured one.
If the TCP optional header is not present in the SYN packet and there are no errors in already present TCP header, the TCP MSS value configured will be inserted while sending the current packet out.

Example

The following command limits the TCP maximum segment size to *3000*, and if not present adds it to the packets:

```
tcp mss 3000 limit-if-present add-if-not-present
```

tcp out-of-order-timeout

Description This command has been deprecated, and is replaced by the tcp packets-out-of-order command.

tcp packets-out-of-order

This command allows you to configure processing of TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

tcp packets-out-of-order { timeout *timeout_duration* **| transmit [after-reordering | immediately] }**

default tcp packets-out-of-order { timeout | transmit }

default

Configures this command with its default setting.

- **timeout**: 5000 milliseconds
- **transmit**: **immediately**

timeout *timeout_duration*

Specifies the timeout duration for re-assembly of TCP out-of-order packets.
timeout_duration is the timeout duration, in milliseconds, and must be an integer from 100 through 30000.
Default: 5000 milliseconds

transmit [after-reordering | immediately]

Configures the TCP out-of-order segment behavior after buffering a copy.

- **after-reordering**: Sends the TCP out-of-order segment after all packets are received and successfully reordered. If reordering is not successful due to a timeout, the received packets are forwarded without being passed through the protocol analyzers. If memory allocation fails or the received packet is partial retransmitted data, the packet will be forwarded immediately without being passed through the protocol analyzers, except for the IP analyzer.
- **immediately**: Sends the TCP out-of-order segment immediately after buffering a copy. The packets are transmitted as they are received without any in-line services or charging action processing, but also a copy of each packet is held onto. When the missing packet is received, complete deep packet inspection of all the packets and all relevant in-line services is done, and then the last packet is forwarded.

Default: **immediately**

Usage

Use this command to configure how to process TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

Example

The following command sets the timeout timer to *10000* milliseconds:

```
tcp packets-out-of-order timeout 10000
```

tcp proxy-mode

This command allows you to enable/disable TCP Proxy mode for all subscribers using the current rulebase.

Product

ACS, CF, MVG, TPO

Privilege

Security Administrator, Administrator

Syntax

```
tcp proxy-mode { dynamic { all | content-filtering | dcca | ip-readdressing | nexthop-readdressing | xheader-insert } + | static [ port [ port_number [ to port_number ] ] ] }

default tcp proxy-mode

no tcp proxy-mode [ dynamic { content-filtering | dcca | ip-readdressing | nexthop-readdressing | xheader-insert } + | static [ port [ port_number [ to port_number ] ] ] ]
```

default

Configures this command with its default setting.
Default: Disabled

no

If previously enabled, disables TCP Proxy mode.
Optionally, TCP Proxy can be disabled for specific options that were previously enabled.

dynamic { all | content-filtering | dcca | ip-readdressing | nexthop-readdressing | xheader-insert } +

Enables TCP proxy for subscriber-initiated TCP flows under the specified condition(s).

- **all**: Specifies that subscriber-initiated TCP flows be proxied if all/any of the following conditions are satisfied.
- **content-filtering**: Specifies that subscriber-initiated TCP flows be proxied if a URL is requested, and that URL is checked because Category-based Content Filtering is enabled in the rulebase.
- **dcca**: Specifies that subscriber-initiated TCP flows be proxied if DCCA is enabled in the charging action.
- **ip-readdressing**: Specifies that subscriber-initiated TCP flows be proxied if IP Readdressing feature is enabled in the charging action.
- **nexthop-readdressing**: Specifies that subscriber-initiated TCP flows be proxied if Nexthop Readdressing feature is enabled in the charging action.
- **xheader-insert**: Specifies that subscriber-initiated TCP flows be proxied if x-Header Insertion feature is enabled in the charging action.

static [port [*port_number* [to *port_number*]]]

Enables static TCP proxy for every subscriber-initiated TCP flow, unless specific ports are specified.
port [*port_number* [to *port_number*]]]
Specifies port numbers and/or range of port numbers.

port_number must be an integer from 1 through 65535.

Important: Up to 32 port numbers and eight port ranges can be specified.

Usage

Important: In release 11.0, TCP Proxy functions only in Static mode. Dynamic TCP Proxy mode is supported only in 12.0 and later releases.

Use this command to enable/disable TCP Proxy mode for all subscribers using this ACS rulebase. Optionally, TCP Proxy can be enabled/disabled for specific ACS features. Note that enabling/disabling the TCP Proxy feature for any of the optional ACS features, does not affect that feature.

Important: Regardless of the setting of this command, TCP Proxy is enabled whenever a TPO profile is selected for the subscriber's flow(s).

Note that the last command overwrites any previous configuration. For example, when the following commands are applied in sequence:

```
tcp proxy-mode dynamic nexthop-readdressing
tcp proxy-mode dynamic xheader-insert
```

The nexthop configuration is overwritten by the x-header configuration.

Example

The following command enables TCP proxy for subscriber-initiated TCP flows whenever next-hop-forwarding-address is configured in the charging action:

```
tcp proxy-mode dynamic nexthop-readdressing
```

tethering-detection

This command allows you to enable/disable the Tethering Detection feature for the current rulebase, and specifies the database to use.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
tethering-detection { os-db-only | ua-db-only }

{ default | no } tethering-detection
```

default

Configures this command with its default setting.
Default: By default, the Tethering Detection feature is disabled. When enabled, unless a specific database is specified to be used, by default tethering detection will make use of both the databases.

no

If previously configured, deletes the tethering detection configuration from the current rulebase.

os-db-only

Specifies to perform tethering detection using only the OS signature database.

ua-db-only

Specifies to perform tethering detection using only the UA signature database.

Usage

Use this command to enable/disable the Tethering Detection feature for a rulebase, and configures the database to use.
Changing the configuration does not affect existing flows of the subscriber. If Tethering Detection was disabled and is turned enabled, it will be applied only to new flows of subscribers using the rulebase.
Also, see the **tethering-database** command in the *ACS Configuration Mode Commands* chapter.

Example

The following command enables the Tethering Detection feature in the rulebase, and specifies to use only the OS database:

```
tethering-detection os-db-only
```

timestamp rounding

This command allows you to enable/disable timestamp rounding in EDRs or eG-CDRs.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
timestamp rounding { edr | egcdr } { ceiling | floor | round-off }

{ default | no } timestamp rounding { edr | egcdr }
```

default

Configures this command with its default setting.
Default: **round-off**

no

Disables timestamp rounding.

edr

Enables timestamp rounding for EDRs.

egcdr

Enables timestamp rounding for eG-CDRs.

ceiling

If the fractional part of the seconds is greater than 0, adds 1 to the number of seconds and discards the fraction.

floor

Discards the fractional part of the second.

round-off

Sets the fractional part of the seconds to nearest integer value. If the fractional value is greater than or equal to 0.5, it adds 1 to the number of seconds and discards the fractional part of second.

Usage

Use this command to configure the timestamp rounding setting.
The specified rounding will be performed before system attempts any calculation. For example using round-off, if the start time is 1.4, and the end time is 1.6, then the calculated duration will be 1 (for example, 2 – 1 = 1).
This command may be repeated for each type of EDR or eG-CDR.

Example

The following command sets the EDR timestamp to nearest integer value second; for example, 34:12.23 to 34:12.00:

```
timestamp rounding edr round-off
```

tpo default-policy

This command allows you to configure the default TPO policy for the current rulebase.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

tpo default-policy *tpo_policy_name*

no tpo default-policy

no

If previously configured, deletes the default TPO policy configuration from the current rulebase.

tpo default-policy *tpo_policy_name*

Specifies the default TPO policy for the current rulebase.
tpo_policy_name must be the name of a TPO policy, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the default TPO policy for a rulebase.
For subscribers using a particular rulebase, the default TPO policy configured in it will be used only if in the APN/subscriber profile no TPO policy is configured, and a policy to use is not received from the AAA/OCS.

Example

The following command configures a TPO policy named *standard* as default TPO policy for the rulebase:

```
tpo default-policy standard
```

transport-layer-checksum

This command allows you to enable/disable checksum verification for TCP and UDP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] transport-layer-checksum verify-during-packet-inspection [ tcp | udp ]

default transport-layer-checksum
```

no

Disables the checksum calculation for the specified packet type.

default

Configures this command with its default setting.
Default: Same as **transport-layer-checksum verify-during-packet-inspection**—to perform the checksum verification calculation on all TCP and UDP packets.

[tcp | udp]

Specifies that either TCP or UDP packets should be verified/not verified.
If neither of these keywords is specified the command applies to both TCP and UDP packets.

Usage

Use this command to disable or enable performing checksum verification calculations on TCP or UDP packets.
If the checksum is not verified, the packets will go through the TCP/UDP analyzers (and deeper analyzers, if so configured via the **route** command) regardless of the value of the TCP/UDP checksum.
If the checksum is verified, only packets with good checksums will go through the TCP/UDP analyzers (and deeper analyzers, if so configured).

Example

The following command disables checksum verification calculations on all TCP and UDP packets:

```
no transport-layer-checksum verify-during-packet-inspection
```

udr threshold

This command allows you to configure the threshold limit to generate Usage Data Records (UDRs) that provide Comma Separated Value (CSV) records written periodically in a fixed schema designed to reflect a total billable quantity.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
udr threshold { interval interval | volume { downlink bytes [ uplink bytes ] | total
bytes | downlink bytes [ uplink bytes ] } }

default udr threshold { interval | volume }

no udr threshold { interval | volume { downlink [ uplink ] | total | uplink [ downlink ]
} }
```

no

If previously configured, deletes the UDR threshold configuration from the current rulebase.

default

Configures this command with its default setting.
Default: Disabled; same as **no udr threshold interval** and **no udr threshold volume**.

interval *interval*

Specifies the time interval, in seconds, for closing the UDR if the minimum time duration thresholds are satisfied. By default, this option is disabled.
interval must be an integer from 60 through 40000000.
Default: 0 (Disabled)

volume

Specifies uplink/downlink volume octet counts for the generation of interim UDRs.

- **downlink** *bytes*: Specifies the limit for the number of downlink octets after which the UDR is closed.

  bytes must be an integer from 100000 through 4000000000.

  Default: 4000000000

- **total** *bytes*: Specifies the limit for the total number of octets (uplink+downlink) after which the UDR is closed.

  bytes must be an integer from 100000 through 4000000000.

  Default: Disabled

- **uplink** *bytes*: Specifies the limit for the number of uplink octets after which the UDR is closed.

  bytes must be an integer from 100000 through 4000000000.

  Default: 4000000000

UDR records are generated whenever either threshold is reached.

Usage

Use this command to enable thresholds for generation of UDRs.

Example

The following command specifies that UDR records should be generated every 10 minutes (*600* seconds):

```
udr threshold interval 600
```

udr trigger

This command allows you to configure additional triggers for generating UDRs.

Important: This command is only available in StarOS 8.3 and later releases.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] udr trigger first-hit-content-id

default udr trigger
```

no

Disables first-hit-content-id UDR trigger.

default

Configures this command with its default setting.
Default: Disabled; no additional triggers.

udr trigger first-hit-content-id

Specifies to generate interim UDR on first packet hit per rating group/content ID.

Usage

This command enables to assign first packet trigger to interim UDRs—for generating UDR for first packet hit per rating group/content ID. The first-hit-content-id trigger when configured causes an UDR to be generated as soon as a packet hits a Charging Action with a content ID. UDR generation will be triggered when this command is configured and present in the rulebase.

Example

The following command assigns first packet trigger to interim UDRs, for generating UDR for first packet hit per rating group/content ID:

```
udr trigger first-hit-content-id
```

url-blacklisting action

This command allows you to enable/disable URL Blacklisting functionality for the current rulebase, and configures the action to be taken when there is a URL match.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

url-blacklisting action { discard | redirect-url *url* **| terminate-flow | www-reply-code-and-terminate-flow** *reply_code* **} [content-id** *content_id* **]**

{ default | no } url-blacklisting action

default

Disables URL Blacklisting in the current rulebase.

no

If previously configured, deletes the URL Blacklisting action configuration from the current rulebase.

discard

Configures URL Blacklisting “discard” action.

redirect-url *url*

Configures URL Blacklisting “redirect-url” action.
url specifies the redirect URL/URI, which must be a fully qualified URL/URI, and must be an alphanumeric string of 1 through 1023 characters.

terminate-flow

Configures URL Blacklisting “terminate-flow” action.

www-reply-code-and-terminate-flow *reply_code*

Configures URL Blacklisting “terminate-flow” action with reply code.
reply_code specifies the reply code, and must be an integer from 100 through 599.

content-id *content_id*

Usage

Use this command to enable/disable URL Blacklisting at the rulebase level, and configure the action to be taken.

Example

The following command enables URL Blacklisting in the rulebase, and configures the terminate-flow action with reply code 300:

```
url-blacklisting action www-reply-code-and-terminate-flow 300
```

The following command disables URL Blacklisting feature in the rulebase:

```
no url-blacklisting action
```

url-preprocessing

This command allows you to enable/disable a group-of-prefixed-urls for preprocessing of embedded URLs.

Important: This command is customer specific. For more information, please contact your Cisco account representative.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] url-preprocessing bypass group-of-prefixed-urls *prefixed_urls_group_name*

no

If previously configured, deletes the URL-preprocessing bypass configuration from the current rulebase.

group-of-prefixed-urls *prefixed_urls_group_name*

Specifies the group-of-prefixed-urls.
prefixed_urls_group_name must be the name of a group-of-prefixed-urls, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to enable/disable a group-of-prefixed-urls for preprocessing of embedded URLs. This command can be issued multiple times to enable multiple groups. If an embedded URL begins with the string specified within any of the groups, that prefix text will be removed from the URL.

Example

The following command enables looking for prefixed URLs of the group-of-prefixed-urls named *test5*:

```
url-preprocessing bypass group-of-prefixed-urls test5
```

wtp out-of-order-timeout

Description This command has been deprecated, and is replaced by the wtp packets-out-of-order command.

wtp packets-out-of-order

This command allows you to configure how to process Wireless Transaction Protocol (WTP) packets that are out of order, while waiting for the earlier packet(s) to arrive.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

wtp packets-out-of-order { out-of-order-timeout *timeout* **| transmit [after-reordering | immediately] }**

default wtp packets-out-of-order { out-of-order-timeout | transmit }

default

Configures this command with its default setting.

- **out-of-order-timeout**: 5000 milliseconds
- **transmit**: **immediately**

out-of-order-timeout *timeout*

Specifies the maximum duration for which WTP out-of-order packets are retained, before reassembly is needed.
timeout is the timeout duration, in milliseconds, and must be an integer from 100 through 30000.
Default: 5000 milliseconds

transmit [after-reordering | immediately]

Specifies the WTP out-of-order segment behavior after buffering a copy:

- **after-reordering**: Sends WTP out-of-order segment after it becomes ordered
- **immediately**: Sends WTP out-of-order segment immediately after buffering a copy

Default: **immediately**

Usage

Use this command to configure TCP out-of-order segment options.
If out-of-order-timeout is specified, out-of-order packets are retained, until either all packets have been received or the configured timeout has expired for the oldest packet. If all packets have been received, a temporary complete packet is reconstructed for analysis. Then all packets are forwarded in order from first to last. If all packets are not received, the packets will be forwarded without being passed through the protocol analyzers, except for the IP analyzer.
If **after-reordering** transmitting is specified, the packets are held onto and reordered. After successfully reordering the packets, they are processed in the proper order. If reordering is not successful due to timeout (wtp out-of-order-timeout), the received packets are forwarded without being passed through the protocol analyzers.
If **immediately** is specified, the packets are transmitted as they are received without any in-line services or Charging Action processing, however a copy of each packet is retained. When the missing packet is received,

complete deep packet inspection of all the packets and all relevant in-line services is undertaken, and then the last packet is forward (unless otherwise configured by the in-line services or Charging Action).

Example

The following command sets the timeout timer to *10000* milliseconds:

```
wtp out-of-order-timeout 10000
```

xheader-encryption

This command allows you to configure X-Header Encryption feature's parameters.

Important: This command is license dependent. For more information, please contact your Cisco account representative.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

xheader-encryption { certificate-name *certificate_name* **| re-encryption period** *period* **}**

default xheader-encryption re-encryption period

no xheader-encryption { certificate-name | re-encryption }

default

Configures this command with its default setting.
Default: Disabled

no

If previously configured, deletes the configuration from the current rulebase.

certificate-name *certificate_name*

Specifies the encryption certificate to use for the X-Header Encryption feature.
certificate_name must be the name of an encryption certificate, and must be an alphanumeric string of 1 through 63 characters.
Default: Disabled; no encryption certificate

re-encryption period *period*

Specifies how often to re-generate the encryption keys.
period specifies the re-encryption time period in minutes, and must be an integer from 1 through 10000.
Default: Disabled; no re-encryption

Usage

Use this command to configure the X-Header Encryption feature's certificate and re-encryption parameters.

Example

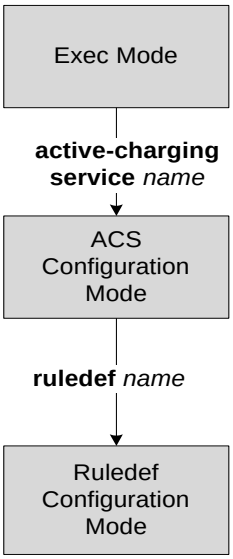
The following command configures the X-Header Encryption feature to use the certificate named *testcert*:

```
xheader-encryption certificate-name testcert
```

Chapter 17
ACS Ruledef Configuration Mode Commands

The ACS Ruledef Configuration Mode is used to create and manage rule expressions in individual rule definitions (ruledefs).

Important: Up to 10 rule expressions can be configured in one ruledef.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

bearer 3gpp apn

This command allows you to define rule expressions to match an Access Point Name (APN) of the bearer flow.

Important: This command is available only in 8.1 and later releases.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

`[ no ] bearer 3gpp apn [ case-sensitive ]` *`operator apn_name`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`apn_name`

Specifies name of the APN to match.
`apn_name` must be an alphanumeric string of 1 through 62 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match an APN in the bearer flow.

Example

The following command defines a rule expression to match user traffic based on APN named *`apn12`*:

```
bearer 3gpp = apn12
```

bearer 3gpp imsi

This command allows you to define rule expressions to match International Mobile Station Identification (IMSI) number in the bearer flow.

Important: This command is available only in 8.1 and later releases.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] bearer 3gpp imsi { *operator imsi* **| { !range | range } imsi-pool** *imsi_pool_name* **}**

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

imsi

Specifies the IMSI number to match.

!range | range

!range | range: Specifies the range criteria:

- **!range**: Not in the range of
- **range**: In the range of

imsi-pool *imsi_pool_name*

Specifies the IMSI pool.
imsi_pool_name must be the name of an IMSI pool, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define rule expressions to match an IMSI.

Example

The following command defines a rule expression to analyze user traffic for the IMSI number *9198838330912*:

```
bearer 3gpp imsi = 9198838330912
```

bearer 3gpp rat-type

This command allows you to define rule expressions to match Radio Access Technology (RAT) in the bearer flow.

Important: This command is available only in 8.1 and later releases.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] bearer 3gpp rat-type` *`operator rat_type`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`=`**: Equals

`rat_type`

Specifies the RAT type to match.
`rat_type` must be one of the following:

- **`geran`**: GSM EDGE Radio Access Network type
- **`utran`**: UMTS Terrestrial Radio Access Network type
- **`wlan`**: Wireless LAN type

Usage

Use this command to define rule expressions to match a RAT type.

Example

The following command defines a rule expression to match user traffic based on RAT type **`wlan`**:

```
bearer 3gpp rat-type = wlan
```

bearer 3gpp sgsn-address

This command allows you to define rule expressions to match SGSN address associated in the bearer flow.

Important: This command is available only in 8.1 and later releases.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] bearer 3gpp sgsn-address *operator ip_address*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

ip_address

Specifies the SGSN IP address to match.
ip_address must be in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to define rule expressions to match IP address of an SGSN node. This command replaces the **bearer sgsn-address** command.

Example

The following command defines a rule expression to analyze user traffic for an SGSN node with IP address *10.1.1.1*:

```
bearer 3gpp sgsn-address = 10.1.1.1
```

bearer 3gpp2 bsid

This command allows you to define rule expressions to match Base Station Identifier (BSID) associated with the bearer.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] bearer 3gpp2 bsid [case-sensitive] use-group-of-objects *operator string*

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

---

use-group-of-objects

Specifies using a group-of-objects as a qualifier to match this rule.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

---

string

Specifies the name of a group-of-objects to match.
If the **use-group-of-objects** keyword is not included in the command, *string* specifies name of the matching 3GPP2 service Base Station ID (BSID) in bearer flow.
If the **use-group-of-objects** keyword is included in the command, *string* must be the name of the group-of-objects to use. In this case, it is checked if the rule is satisfied for either one or none of the objects in the group-of-objects depending upon the operator used. For example, if the *operator* is **contains**, the expression would be true if any of the objects in the specified object group is contained in the BSID. If the *operator* is **!contains**, then the expression would be true if none of the objects in the object group is contained in the BSID.
string must be an alphanumeric string of 1 through 16 characters, and may contain punctuation characters.

Usage

Use this command to define rule expressions to match a 3GPP2 Base Station Identifier (BSID).

Example

The following command defines a rule expression to analyze user traffic for 3GPP2 BSID named *bs001_xyz*:

```
bearer 3gpp2 bsid = bs001_xyz
```

bearer 3gpp2 service-option

This command allows you to define rule expressions to match 3GPP2 service with service options associated with the bearer.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] bearer 3gpp2 service-option *operator service_option_code*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

service_option_code

Specifies the 3GPP2 service option code to match.
*service_option_code*must be an integer from 0 through 1000.

Usage

Use this command to define rule expressions to match a 3GPP2 service's service option code.

Example

The following command defines a rule expression to analyze user traffic for a 3GPP2 service's service option matching *1034*:

```
bearer 3gpp2 service-option = 1034
```

bearer apn

This command allows you to define rule expressions to match the APN used for the subscriber session.

Important: In 8.1 and later releases, this command is deprecated and is replaced by the bearer 3gpp apn command.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

`[ no ] bearer apn [ case-sensitive ]` *`operator apn_name`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`apn_name`

Specifies the APN to match.
`apn_name` must be the name of an APN, and must be an alphanumeric string of 1 through 62 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match APN used for subscriber session.

Example

The following command defines a rule expression to match user traffic based on APN name *`apn12`*:

```
bearer apn = apn12
```

bearer imsi

This command allows you to define rule expressions to match IMSI number of the subscriber.

Important: In 8.1 and later releases, this command is deprecated and is replaced by the bearer 3gpp imsi command.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] bearer imsi {` *`operator imsi`* **`| { !range | range } imsi-pool`** *`imsi_pool_name`* **`}`**

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`=`**: Equals

`imsi`

Specifies the IMSI number to match.

`!range | range`

Specifies the range criteria:

- **`!range`**: Not in the range of
- **`range`**: In the range of

`imsi-pool` *`imsi_pool_name`*

Specifies an IMSI pool.
`imsi_pool_name` must be the name of an IMSI pool, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define rule expressions to match IMSI number of subscriber.

Example

The following command defines a rule expression to match user traffic based on IMSI number *`9198838330912`*:

```
bearer imsi = 9198838330912
```

bearer rat-type

This command allows you to define rule expressions to match Radio Access Technology (RAT) in the bearer flow.

Important: In 8.1 and later releases, this command is deprecated and is replaced by the bearer 3gpp rat-type command.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] bearer rat-type *operator rat_type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

rat_type

Specifies the RAT type to match.
rat_type must be one of the following:

- **geran**: GSM EDGE Radio Access Network type
- **utran**: UMTS Terrestrial Radio Access Network type
- **wlan**: Wireless LAN type

Usage

Use this command to define rule expressions to match a RAT type.

Example

The following command defines a rule expression to match user traffic based on RAT type **wlan**:

```
bearer rat-type = wlan
```

bearer sgsn-address

This command allows you to define rule expressions to match IP address of the SGSN (in acting as GGSN) / P-GW (if acting as S-GW) in the bearer flow.

Important: In 8.1 and later releases, this command is deprecated and is replaced by the bearer 3gpp sgsn-address command.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] bearer sgsn-address` *`operator address`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`=`**: Equals

`address`

Specifies the SGSN IP address to match.
`address` must be in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to define rule expressions to match IP address of the SGSN (in acting as GGSN) / P-GW (if acting as S-GW).

Example

The following command defines a rule expression to match user traffic based on SGSN node IP address *`10.1.1.1`*:

```
bearer sgsn-address = 10.1.1.1
```

bearer traffic-group

This command allows you to define rule expressions to match traffic group number associated with the subscriber session.

Important: This functionality is available only if the Content Access Control license has been installed on the chassis.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] bearer traffic-group` *`operator group_number`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`<=`**: Lesser than or equals
- **`=`**: Equals
- **`>=`**: Greater than or equals

`group_number`

Specifies the traffic group number to match.
`group_number` must be an integer from 1 through 255.

Usage

Use this command to define rule expressions to match traffic group of the subscriber session. See the **`fa-ha-spi`** command in the *HA Service Configuration Mode Commands* chapter for more information.

Example

The following command defines a rule expression to analyze all traffic groups assigned a value greater or equal to *`23`*:

```
bearer traffic-group >= 23
```

cca quota-state

Specifies the quota state of a subscriber for prepaid credit control service. Release 12.0 onwards, this command should be used as a post-processing rule. For more information on post-processing policy command, refer to the *ACS Rulebase Configuration Mode Commands* chapter in this guide.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] cca quota-state operator { limit-reached | lower-bandwidth }
```

no

Disables the configured credit control quota state.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

limit-reached

This state matches an affirmative end-of-quota indication for the current ruledef from the prepay server.

lower-bandwidth

This state matches the lower-bandwidth quota state of a rating group.

Usage

This command supports URL redirection and creates a rule for subscriber prepaid quota state as exhausted or not exhausted.
If a subscriber has exhausted the quota but has not exhausted the qualified period, a different charging-action can be applied via the **cca quota-state** command.

Example

The following command defines a rule expression to match user traffic based on the Credit-Control Application (CCA) quota state **limit-reached**:

```
cca quota-state = limit-reached
```

cca redirect-indicator

This command allows you to define rule expressions to match redirect-indicator state of the Credit Control Application. Release 12.0 onwards, this command should be used as a post-processing rule. For more information on post-processing policy command, refer to *ACS Rulebase Configuration Mode Commands* chapter in this reference.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] cca redirect-indicator` *`operator redirect_indicator`*

`no`

Disables the configured CCA redirect-indicator in the current ruledef.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`<=`**: Lesser than or equals
- **`=`**: Equals
- **`>=`**: Greater than or equals

`redirect_indicator`

Specifies the redirect indicator for the AVP used for redirection of the URL in the RADIUS dictionary for prepaid service. It must be an integer from 0 through 4294967295.

Important: For the RADIUS server configured with different values to return for this AVP, the ACS requires ruledefs to match the different values for system to associate with charging actions that have different redirect URLs configured.

Usage

This command is used to configure an AVP to be used from a dictionary that defines the AVP for the redirect-indicator.
For example, a RADIUS dictionary specifies the 3gpp2-release-indicator to be used for the redirect indicator when RADIUS is used as the Credit-Control Application. In this case, the value for 3gpp2-release-indicator that is returned by the RADIUS prepaid server for a quota request for a given content ID is retained by system and associated with the flow.

Example

The following command defines a rule expression to match redirect indicator *`1234`* for the URL Redirect AVP:

```
cca redirect-indicator = 1234
```

copy-packet-to-log

This command allows you to print every packet that hits the current ruledef to a log statement.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] copy-packet-to-log
```

no

Disables the copy-packet-to-log feature.

copy-packet-to-log

Specifies to print packets hitting the current ruledef to a log.

Usage

Use this command to print every packet that hits a ruledef to a log statement. This facilitates debugging.

dns answer-name

This command allows you to define rule expressions to match answer name in the answer section of DNS response messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] dns answer-name [ case-sensitive ]` *`operator value`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`value`

Specifies the value to match.
`value` must be an alphanumeric string of 1 through 255 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match an answer name from the answer section of DNS response messages.
The answer section of a DNS response may contain more than one answer. A maximum of seven answers from the response packet are parsed. For the equality expressions (=, contains, starts-with, ends-with) a match is sought from any of the answers in the packet (up to the first seven answers). For the inequality expressions (!=, !contains, !starts-with, !ends-with), a non-match is sought from all answers (up to the first seven answers).

Example

The following command defines a rule expression to match user traffic for answer name *test*:

```
dns answer-name = test
```

dns any-match

This command allows you to define rule expressions to match all DNS packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] dns any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define an any-match rule expression to match all DNS packets.

Example

The following command defines an any-match rule expression to match all DNS packets:

```
dns any-match = TRUE
```

dns previous-state

This command allows you to define rule expressions to match previous state of the DNS FSM.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] dns previous-state *operator dns_previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

dns_previous_state

Specifies the previous state to match.
dns_previous_state must be one of the following:

- **dns-timeout**
- **init**
- **req-sent**
- **resp-error**
- **resp-success**

Usage

Use this command to define rule expressions to match previous state of DNS FSM.

Example

The following command defines a rule expression to match the DNS FSM previous state **req-sent**:

```
dns previous-state = req-sent
```

dns query-name

This command allows you to define rule expressions to match query name in DNS request messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] dns query-name [case-sensitive] *operator query_name*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

query_name

Specifies the query name to match.
query_name must be an alphanumeric string of 1 through 255 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match query name in DNS request messages.

Example

The following command defines a rule expression to match DNS query name *test*:

```
dns query-name = test
```

dns return-code

This command allows you to define rule expressions to match response code in DNS response messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] dns return-code *operator return_code*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

return_code

Specifies the response code to match.
return_code must be one of the following:

- **format-error**
- **name-error**
- **no-error**
- **not-implemented**
- **refused**
- **server-failure**

Usage

Use this command to define rule expressions to match response code in DNS response messages.

Example

The following command defines a rule expression to match a DNS response code **refused**:

```
dns return-code = refused
```

dns state

This command allows you to define rule expressions to match current state of DNS FSM.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] dns state *operator dns_current_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

dns_current_state

Specifies the current state to match.
dns_current_state must be one of the following:

- **dns-timeout**
- **init**
- **req-sent**
- **resp-error**
- **resp-success**

Usage

Use this command to define rule expressions to match DNS FSM current state.

Example

The following command defines a rule expression to match DNS FSM current state of **req-sent**:

```
dns state = req-sent
```

dns tid

This command allows you to define rule expressions to match Transaction Identifier (TID) field in DNS messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] dns tid *operator tid_value*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

tid_value

Specifies the DNS transaction identifier to match.
tid_value must be an integer from 1 through 65535.

Usage

Use this command to define rule expressions to match a TID field of DNS messages.

Example

The following command defines a rule expression to match DNS TID field value of *test*:

```
dns tid = test
```

email

This command allows you to define rule expressions to match generic e-mail message parameters. These expressions will be applicable for IMAP, MMS, POP3, and SMTP protocols.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] email { cc | content { class | type } | from | size | subject | to } [ case-sensitive ]` *`operator value`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`cc`

Specifies to match the “cc” field of standard e-mail message.

`content { class | type }`

Specifies to match the “content-type” or “content-class” field of standard e-mail message.

`from`

Specifies to match the “from” field of standard e-mail message.

`subject`

Specifies to match the “subject” field of standard e-mail message.

`to`

Specifies to match the “to” field of standard e-mail message.

`size`

Specifies to match with the total size of e-mail message specified in bytes.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following except for **`size`**:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with

- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

operator must be one of the following for **size**:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

value

Specifies the value to match.
value must be an alphanumeric string and can contain punctuation characters.

- **cc**: A string of 1 through 512 characters
- **content**: A string of 1 through 128 characters
- **from**: A string of 1 through 64 characters
- **size**: A range of bytes from 1 through 4000000000 bytes
- **subject**: A string of 1 through 128 characters
- **to**: A string of 1 through 512 characters

Usage

Use this command to define rule expressions to match different fields/parameters within standard e-mail messages.

Example

The following command defines a rule expression to analyze user traffic for the occurrence of *triangle* in the “cc” field of e-mail messages:

```
email cc contains triangle@xyz.com
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

file-transfer any-match

This command allows you to define rule expressions to match all file-transfer packets. This expression applies to file transfers that use the FTP or HTTP protocols.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] file-transfer any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all file-transfer packets. This expression applies to file transfers that use the FTP or HTTP protocols.

Example

The following command defines a rule expression to match all file-transfer packets:

```
file-transfer any-match = TRUE
```

file-transfer chunk-number

This command allows you to define rule expressions to match the total number of chunks in an HTTP file as determined by the File Transfer analyzer.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] file-transfer chunk-number *operator chunks_number*

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

---

chunks_number

Specifies the number of chunks to match.
chunks_number must be an integer from 1 through 65535.

Usage

Use this command to define rule expressions to match the total number of chunks in an HTTP file as determined by the File Transfer analyzer.

Example

The following command defines a rule expression to match *150* number of chunks:

```
file-transfer chunk-number = 150
```

file-transfer current-chunk-length

This command allows you to define rule expressions to match the length of an HTTP chunk currently in the File Transfer analyzer.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] file-transfer current-chunk-length *operator current_chunk_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

current_chunk_length

Specifies the current chunk length value (in bytes) to match.
current_chunk_length must be an integer from 1 through 40000000.

Usage

Use this command to define rule expressions to match the length of an HTTP chunk currently in the File Transfer analyzer.

Example

The following command defines a rule expression to match length of current HTTP chunk as *1500000* bytes:

```
file-transfer current-chunk-length = 1500000
```

file-transfer declared-chunk-length

This command allows you to define rule expressions to match the declared length of an HTTP chunk currently in the File Transfer analyzer.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] file-transfer declared-chunk-length *operator declared_chunk_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

declared_chunk_length

Specifies the declared chunk length value (in bytes) to match.
declared_chunk_length must be an integer from 1 through 40000000.

Usage

Use this command to define rule expressions to match the declared length of an HTTP chunk currently in the File Transfer analyzer.

Example

The following command defines a rule expression to match declared length of the current HTTP chunk as *2500000* bytes:

```
file-transfer declared-chunk-length = 2500000
```

file-transfer declared-file-size

This command allows you to define rule expressions to match the declared file size by the File Transfer analyzer decoding the FTP handshake.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] file-transfer declared-file-size *operator declared_file_size*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

declared_file_size

Specifies the declared file size (in bytes) to match.
declared_file_size must be an integer from 1 through 40000000.

Usage

Use this command to define rule expressions to match the declared file size by the File Transfer analyzer decoding the FTP handshake.

Example

The following command defines a rule expression to match declared file size as *2500000* bytes:

```
file-transfer declared-file-size = 2500000
```

file-transfer filename

This command allows you to define rule expressions to match file name.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] file-transfer filename [ case-sensitive ]` *`operator file_name`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`file_name`

Specifies the file name to match.
`file_name` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match file name in file-transfer.

Example

The following command defines a rule expression to match file name containing *`star1`*:

```
file-transfer filename contains star1
```

file-transfer previous-state

This command allows you to define rule expressions to match previous state of File Transfer FSM.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] file-transfer previous-state *operator file_transfer_previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

file_transfer_previous_state

Specifies the previous state to match.
file_transfer_previous_state must be one of the following:

- **init**: Specifies previous state as initialization.
- **request-sent**: Specifies previous state as request sent.
- **transfer-error**: Specifies previous state as transfer error.
- **transfer-ok**: Specifies previous state as transfer ok.

Usage

Use this command to define rule expressions to match previous state of File Transfer FSM.

Example

The following command defines a rule expression to match previous state of **init**:

```
file-transfer previous-state = init
```

file-transfer state

This command allows you to define rule expressions to match the current state of File Transfer FSM.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] file-transfer state *operator file_transfer_current_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

file_transfer_current_state

Specifies the current state to match.
file_transfer_current_state must be one of the following

- **init**: Specifies current state as initialization.
- **request-sent**: Specifies current state as request sent.
- **transfer-error**: Specifies current state as transfer error.
- **transfer-ok**: Specifies current state as transfer ok.

Usage

Use this command to define rule expressions to match current state of File Transfer FSM.
The following table describes details of File Transfer FSM states with event:

Event	init	request-sent	transfer-ok	transfer-err
FTP “RETR” command or HTTP “GET” request received with chunk encoding	request-sent	Discarded	Discarded	Discarded
HTTP 2xx response received	transfer-ok	Discarded	Discarded	Discarded
HTTP 4xx or HTTP 5xx response received	transfer-error	Discarded	Discarded	Discarded
FTP reply received with reply status as file-transfer complete/successful	Discarded	transfer-ok	Discarded	Discarded
FTP reply received with reply status as file-transfer unsuccessful	Discarded	transfer-error	Discarded	Discarded

Example

The following command defines a rule expression to match file-transfer current state of **init**:

```
file-transfer state = init
```

file-transfer transferred-file-size

This command allows you to define rule expressions to match the size of a file that has been transferred so far, as detected by the File Transfer analyzer.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] file-transfer transferred-file-size *operator transferred_file_size*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

transferred_file_size

Specifies the transferred file size (in bytes) to match.
transferred_file_size must be an integer from 1 through 4000000000.

Usage

Use this command to define rule expressions to match the size of the file that has been transferred so far, as detected by the File Transfer analyzer.

Example

The following command defines a rule expression to match file transferred size of *2500* bytes:

```
file-transfer transferred-file-size = 2500
```

ftp any-match

This command allows you to define rule expressions to match all FTP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define a rule expression to match all FTP packets.

Example

The following command defines a rule expression to match all FTP packets:

```
ftp any-match = TRUE
```

ftp client-ip-address

This command allows you to define rule expressions to match IP address of the FTP client.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp client-ip-address *operator ip_address*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

ip_address

Specifies the FTP client IP address to match.
ip_address must be in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to define rule expressions to match an FTP client IP address, which will be either the IP source address or the IP destination address, depending on the direction.

Example

The following command defines a rule expression to match client IP address *10.1.1.1*:

```
ftp client-ip-address = 10.1.1.1
```

ftp client-port

This command allows you to define rule expressions to match port number of the FTP client.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp client-port *operator port_number*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

port_number

Specifies the client port number to match.
port_number must be an integer from 1 through 65535.

Usage

Use this command to define rule expressions to match port number of the FTP client, which will be either the TCP source port or the TCP destination port, depending on the direction.

Example

The following command defines a rule expression to match FTP client port number *10*:

```
ftp client-port = 10
```

ftp command args

This command allows you to define rule expressions to match arguments within an FTP command.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp command args [case-sensitive] *operator argument*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

argument

Specifies the argument to match.
argument must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match arguments within an FTP command.

Example

The following command defines a rule expression to match argument *ascii* within an FTP command:

```
ftp command args = ascii
```

ftp command id

This command allows you to define rule expressions to match FTP command ID.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp command id *operator command_id*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

command_id

Specifies the command identifier to match.
In 8.3 and earlier releases, *command_id* must be an integer from 0 through 15.
In 9.0 and later releases, *command_id* must be an integer from 0 through 18.

Usage

Use this command to define rule expressions to match FTP command ID.

Example

The following command defines a rule expression to match the FTP command ID *10*:

```
ftp command id = 10
```

ftp command name

This command allows you to define rule expressions to match FTP command name.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp command name *operator command_name*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

command_name

Specifies the command name to match.
command_name must be one of the following:

- **abor**: Abort command
- **cwd**: Current working directory command
- **eprt**: eprt command
- **epsv**: epsv command
- **list**: List command
- **mode**: Transfer mode command
- **pass**: Password command
- **pasv**: Passive command
- **port**: Port command
- **quit**: Quit command
- **rest**: Restore command
- **retr**: Retry command
- **stor**: Store command
- **stru**: File structure command
- **syst**: System command
- **type**: Type command
- **user**: User command

Usage

Use this command to define rule expressions to match FTP command name.

Example

The following command defines a rule expression to match FTP command name **list**:

```
ftp command name = list
```

ftp connection-type

This command allows you to define rule expressions to match FTP connection type.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp connection-type *operator connection_type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

connection_type

Specifies the connection type to match.
connection_type must be one of the following:

- **0**: Unknown
- **1**: Control connection
- **2**: Data connection

Usage

Use this command to define rule expressions to match an FTP connection type.

Example

The following command defines a rule expression to match FTP connection type **1**:

```
ftp connection-type = 1
```

ftp data-any-match

This command allows you to define rule expressions to match all FTP data packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp data-any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all FTP data packets.

Example

The following command defines a rule expression to match all FTP data packets:

```
ftp data-any-match = TRUE
```

ftp filename

This command allows you to define rule expressions to match FTP file name.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp filename [case-sensitive] *operator file_name*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

file_name

Specifies the file name to match.
file_name must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match an FTP file name.

Example

The following command defines a rule expression to match a file named *testtransfer*:

```
ftp filename = testtransfer
```

ftp pdu-length

This command allows you to define rule expressions to match the length of a current FTP packet.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp pdu-length *operator pdu_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

pdu_length

Specifies the FTP PDU length (in bytes) to match.
pdu_length must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match the length of a current FTP packet, that is, FTP PDU length (FTP header + FTP payload).

Example

The following command defines a rule expression to match an FTP PDU length of *9647* bytes:

```
ftp pdu-length = 9647
```

ftp pdu-type

This command allows you to define rule expressions to match FTP Protocol Data Unit (PDU) type.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp pdu-type *operator pdu_type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

pdu_type

Specifies the PDU type to match.
pdu_type must be one of the following:

- **0**: Unknown
- **1**: Command
- **2**: Reply

Usage

Use this command to define rule expressions to match a PDU type of FTP packet.

Example

The following command defines a rule expression to match FTP PDU type **1**:

```
ftp pdu-type = 1
```

ftp previous-state

This command allows you to define rule expressions to match previous state of FTP session.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp previous-state *operator ftp_previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

ftp_previous_state

Specifies the previous state to match.
ftp_previous_state must be one of the following:

- **command-sent**
- **init**
- **response-error**
- **response-ok**

Usage

Use this command to define rule expressions to match a previous state of FTP session.

Example

The following command defines a rule expression to match previous FTP state **init**:

```
ftp previous-state = init
```

ftp reply code

This command allows you to define rule expressions to match FTP reply code.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp reply code *operator reply_code*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

reply_code

Specifies the FTP reply code to match.
reply_code must be an integer from 100 through 599.

Usage

Use this command to define rule expressions to match an FTP reply code.

Example

The following command defines a rule expression to match FTP reply code *150*:

```
ftp reply code = 150
```

ftp server-ip-address

This command allows you to define rule expressions to match FTP server IP address.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp server-ip-address *operator ip_address*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

ip_address

Specifies IP address of the server to match
ip_address must be in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to define rule expressions to match an FTP server IP address, which will be either the IP source address or the IP destination address, depending on the direction.

Example

The following command defines a rule expression to match the FTP server IP address *10.1.1.1*:

```
ftp server-ip-address = 10.1.1.1
```

ftp server-port

This command allows you to define rule expressions to match FTP server port number.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp server-port *operator port*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

port

Specifies the FTP server port number to match.
port must be an integer from 1 through 65535.

Usage

Use this command to define rule expressions to match an FTP server port number, which will be either the TCP source port or the TCP destination port, depending on the direction.

Example

The following command defines a rule expression to analyze user traffic for FTP server port *21*:

```
ftp server-port = 21
```

ftp session-length

This command allows you to define rule expressions to match the total number of bytes sent on an FTP control connection.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp session-length *operator session_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

session_length

Specifies the FTP session length (in bytes) to match.
session_length must be an integer from 1 through 4000000000.

Usage

Use this command to define rule expressions to match the total number of bytes sent on an FTP control connection.

Example

The following command defines a rule expression to match FTP session length of *40000* bytes:

```
ftp session-length = 40000
```

ftp state

This command allows you to define rule expressions to match the current state of an FTP session.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp state *operator* **{ close | command-sent | init | response-error | response-ok }**

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

close

Specifies FTP transmissions that are in closed state.

command-sent

Specifies FTP transmissions that are in command-sent state.

init

Specifies FTP transmissions that are in initialized state.

response-error

Specifies FTP transmissions that are in response-error state.

response-ok

Specifies FTP transmissions that are in response-ok state.

Usage

Use this command to define rule expressions to match the current state of an FTP session.

Example

The following command defines a rule expression to match FTP current state **close**:

```
ftp state = close
```

ftp url

This command allows you to define rule expressions to match the FTP URL/path of a file being transferred.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp url [case-sensitive] *operator url*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

url

Specifies the URL to match.
url must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match the FTP URL/path of a file being transferred.

Example

The following command defines a rule expression to match the URL *ftp://rfc.ietf.org/rfc/rfc1738.txt*:

```
ftp url = ftp://rfc.ietf.org/rfc/rfc1738.txt
```

ftp user

This command allows you to define rule expressions to match the user name FTP command packet.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ftp user [case-sensitive] *operator ftp_user*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

ftp_user

Specifies the FTP user name to match.
ftp_user must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match a user name FTP command.

Example

The following command defines a rule expression to match FTP user name *user1*:

```
ftp user = user1
```

http any-match

This command allows you to define rule expressions to match all HTTP and HTTPs Connect Method packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all HTTP packets.

Example

The following command defines a rule expression to match all HTTP packets:

```
http any-match = TRUE
```

http attribute-in-data

This command allows you to define rule expressions to match any arbitrary attribute in the payload following the HTTP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http attribute-in-data *attribute* **[case-sensitive]** *operator value*

no

If previously configured, deletes the specified rule expression from the current ruledef.

attribute

attribute must be an alphanumeric string of 1 through 31 characters.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

value

Specifies the value as an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match arbitrary attribute in the payload following the HTTP headers.

http attribute-in-url

This command allows you to define rule expressions to match arbitrary attribute in the combined Host+URI HTTP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http attribute-in-url *attribute* **[case-sensitive]** *operator value*

no

If previously configured, deletes the specified rule expression from the current ruledef.

attribute

attribute must be an alphanumeric string of 1 through 31 characters.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

value

Specifies the value as an alphanumeric string of 1 through 127 characters.

Usage

Use this command to configure rule expression to match an arbitrary attribute in the combined Host+URI HTTP headers.

http content disposition

This command allows you to define rule expressions to match optional content-disposition field of HTTP entity header.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http content disposition [case-sensitive] *operator content_disposition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

content_disposition

This field offers a mechanism for the sender to transmit presentational information to the recipient, allowing each component of a message to be tagged with an indication of its desired presentation semantics.
content_disposition must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

Usage

Use this command to define rule expressions to match optional content-disposition field of HTTP entity header. This feature supports RFC 2616 for HTTP and RFC 1806 for Content Disposition.

Example

The following command defines a rule expression to match content disposition *successful*:

```
http content disposition = successful
```

http content length

This command allows you to define rule expressions to match the value in HTTP Content-Length entity-header field.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http content length *operator content_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

content_length

Specifies the HTTP body length (in bytes) to match.
content_length must be an integer from 1 through 4000000000.

Usage

Use this command to define rule expressions to match value in HTTP Content-Length entity-header field.

Example

The following command defines a rule expression to match value of *10000* bytes in HTTP Content-Length entity-header field:

```
http content length = 10000
```

http content type

This command allows you to define rule expressions to match value in HTTP Content-Type entity-header field.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] http content type [ case-sensitive ]` *`operator content_type`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`content_type`

Specifies the content type to match.
`content_type` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match value in HTTP Content-Type entity-header field.

Example

The following command defines a rule expression to match *`abc100`* in HTTP Content-Type entity-header field:

```
http content type = abc100
```

http domain

This command allows you to define rule expressions to match the domain portion of URIs in HTTP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http domain [case-sensitive] *operator domain*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

domain

Specifies the domain to match.
domain must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match the domain portion of URIs in HTTP packets. From the URL, after http:// (if present) is removed, everything until the first "/" is the domain.

Example

The following command defines a rule expression to match user traffic based on domain name *testdomain*:

```
http domain = testdomain
```

http error

This command allows you to define rule expressions to match for errors in HTTP packets (for example, invalid HTTP header) and errors in the HTTP analyzer FSM (Finite State Machine) while parsing HTTP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http error *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match for errors in HTTP packets and other errors in HTTP analyzer FSM while parsing HTTP packets. For example, FSM error, invalid header field values, ACS memory and buffer limit, packet related errors, and so on.
ACS supports pipelining of up to 32 HTTP requests on the same TCP connection. Pipeline overflow requests are not analyzed. Such overflow requests are treated as HTTP error. The billing system, based on this information, decides to charge or not charge, or refund the subscriber accordingly.

Example

The following command defines a rule expression to match user traffic based on HTTP error status of **TRUE**:

```
http error = TRUE
```

http first-request-packet

This command allows you to define rule expressions to match the GET or POST request, if it is the first HTTP request for the subscriber's session.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http first-request-packet *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match the GET or POST request, if it is the first HTTP request for the subscriber's session.
This expression can be connected with a charging action, so the subscriber is redirected to a splash page for the first Web access attempted.

Example

The following command defines a rule expression to match first-request-packet:

```
http first-request-packet = TRUE
```

http header-length

This command allows you to define rule expressions to match HTTP header length.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http header-length *operator header_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

header_length

Specifies the HTTP header length (in bytes) to match.
header_length must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match the length of an HTTP header.

Example

The following command defines a rule expression to match an HTTP header length of *8000*:

```
http header-length = 8000
```

http host

This command allows you to define rule expressions to match value in HTTP Host request-header field.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http host [case-sensitive] *operator host_name*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

host_name

Specifies the host name to match.
host_name must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match value in HTTP Host request-header field.

Example

The following command defines a rule expression to match *host1* in HTTP Host request-header field:

```
http host = host1
```

http payload-length

This command allows you to define rule expressions to match HTTP payload length.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http payload-length *operator payload_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

payload_length

Specifies the HTTP payload (data) length (in bytes) to match.
payload_length must be an integer from 1 through 4000000000.

Usage

Use this command to define rule expressions to match an HTTP payload (data) length (pdu-length - header-length).

Example

The following command defines a rule expression to match an HTTP payload length of *100000* bytes:

```
http payload-length = 100000
```

http pdu-length

This command allows you to define rule expressions to match the total length of a single HTTP packet.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http pdu-length *operator pdu_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

pdu_length

Specifies the HTTP PDU length (in bytes) to match.
pdu_length must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match the total length of a single HTTP packet. This will also match packets with partial HTTP message (due to fragmentation).

Example

The following command defines a rule expression to match an HTTP PDU length of *10000* bytes:

```
http pdu-length = 10000
```

http previous-state

This command allows you to define rule expressions to match previous state of HTTP sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http previous-state *operator http_previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

http_previous_state

Specifies the previous state to match.
http_previous_state must be one of the following:

- **init**: Initialized state
- **response-error**: Response error state
- **response-ok**: Response ok state
- **waiting-for-response**: Waiting for response state

Usage

Use this command to define rule expressions to match a previous state of HTTP sessions.

Example

The following command defines a rule expression to match HTTP previous state **response-ok**:

```
http previous-state = response-ok
```

http referer

This command allows you to define rule expressions to match the value in the HTTP Referer request-header field.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http referer [case-sensitive] *operator referer_name*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

referer_name

Specifies the HTTP referer name to match.
referer_name must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match value in HTTP Referer request-header field.
This feature allows an operator to collect or track all URLs visited during a particular subscriber session. These URLs include the entire string of visited URLs, including all referral links. This information is output in an Event Data Record (EDR) format to support reporting or billing functions.
For example, if a subscriber begins a mobile web session and clicks on the “Sports” link from the home deck, and then selects ESPN and moves to an advertiser link, the operator can capture all URLs for that entire session. During this period ACS collects the URLs for a particular subscriber session; collection can be limited by time duration or number of URLs visited.

Example

ACS generates EDRs that contain HTTP URL and the HTTP referer fields along with other fields.

The following command defines a rule expression to match the HTTP referer *cricket.espn.com*:

```
http referer = cricket.espn.com
```

http reply code

This command allows you to define rule expressions to match status code associated with HTTP response packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http reply code *operator reply_code*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

reply_code

Specifies the HTTP reply code to match.
reply_code must be an integer from 100 through 599.

Usage

Use this command to define rule expressions to match status code associated with HTTP response codes.

Example

The following command defines a rule expression to match HTTP response code *204*:

```
http reply code = 204
```

http request method

This command allows you to define rule expressions to match HTTP request method.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http request method *operator request_method*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

request_method

Specifies the HTTP request method to match.
request_method must be one of the following:

- **connect**
- **delete**
- **get**
- **head**
- **options**
- **post**
- **put**
- **trace**

Usage

Use this command to define rule expressions to match an HTTP request method.

Example

The following command defines a rule expression to match user traffic based on HTTP request method **connect**:

```
http request method = connect
```

http session-length

This command allows you to define rule expressions to match HTTP session length.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http session-length *operator session_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

session_length

Specifies the HTTP total session length (in bytes) to match.
session_length must be an integer from 1 through 4000000000.

Usage

Use this command to define rule expressions to match a total HTTP session length.

Example

The following command defines a rule expression to match an HTTP session length of *200000*:

```
http session-length = 200000
```

http state

This command allows you to define rule expressions to match current state of an HTTP session.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http state *operator current_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

current_state

Specifies the current state of HTTP session to match.
current_state must be one of the following:

- **close**: Closed state
- **response-error**: Response error state
- **response-ok**: Response ok state
- **waiting-for-response**: Waiting for response state

Usage

Use this command to define rule expressions to match a current state of an HTTP session.

Example

The following command defines a rule expression to match current state **close**:

```
http state = close
```

http transaction-length

This command allows you to define rule expressions to match HTTP transaction length (combined length of one HTTP GET Request message and its associated response messages).

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http transaction-length { *operator transaction_length* **| { { range | !range }** *range_from* **to** *range_to* **} }**

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

transaction_length

Specifies the HTTP transaction length (in bytes) to match.
transaction_length must be an integer from 1 through 4000000000.

{ range | !range } *range_from* **to** *range_to*

Enables or disables the range criteria for length of transaction.

- **range**: Enables the range criteria for HTTP transaction length.
- **!range**: Disables the range criteria for HTTP transaction length.
- *range_from*: Specifies the start of range (in bytes) for HTTP transaction length.
- *range_to*: Specifies the end of range (in bytes) for HTTP transaction length.

Usage

Use this command to define rule expressions to match an HTTP transaction length [one HTTP GET Request message + associated response message(s)] in bytes.

Example

The following command defines a rule expression to match an HTTP transaction length of *10200* bytes:

```
http transaction-length = 10200
```

http transfer-encoding

This command allows you to define rule expressions to match the value in HTTP Transfer-Encoding general-header field.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http transfer-encoding [case-sensitive] *operator transfer_encoding*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

transfer_encoding

Specifies the HTTP transfer encoding to match.
transfer_encoding must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the value in HTTP Transfer-Encoding general-header field.

Example

The following command defines a rule expression to match the value *chunked* in HTTP Transfer-Encoding general-header field:

```
http transfer-encoding = chunked
```

http uri

This command allows you to define rule expressions to match HTTP URI.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http uri [case-sensitive] *operator uri*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

uri

Specifies the HTTP URI to match.
uri must be an alphanumeric string of 1 through 127 characters, and can contain punctuation characters, and excludes the “host” portion.

Usage

Use this command to define rule expressions to match an HTTP URI, excluding the host portion.

Example

The following command defines a rule expression to match the HTTP URI string *http://www.somehost.com*:

```
http uri = http://www.somehost.com
```

http url

This command allows you to define rule expressions to match HTTP URL.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http url [case-sensitive] *operator url*

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

---

url

Specifies the HTTP URL to match.
url must be an alphanumeric string of 1 through 127 characters. that allows punctuation characters and includes “host + URI” for HTTP PDUs.
For example, in case of the URL “http://www.google.fr/”, the host is “http://www.google.fr”, and the URI is “/”:

```
Hypertext Transfer Protocol
 GET / HTTP/1.1\r\n
 Request Method: GET
 Request URI: /
 Request Version: HTTP/1.1
```

```
Accept: */*\r\n

Accept-Language: fr\r\n

Accept-Encoding: gzip, deflate\r\n

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)\r\n

Host: www.google.fr\r\n

Connection: Keep-Alive\r\n

\r\n
```

Usage

Use this command to define rule expressions to match HTTP URL.

Example

The following command defines a rule expression to match the HTTP URL *http://rfc.ietf.org/rfc/rfc1738.txt*:

```
http url = http://rfc.ietf.org/rfc/rfc1738.txt
```

http user-agent

This command allows you to define rule expressions to match the User-Agent request-header field of HTTP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http user-agent [case-sensitive] *operator user_agent*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

user_agent

Specifies the HTTP user agent value to match.
user_agent must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match value in HTTP user-agent header field.

Example

The following command defines a rule expression to match *xyz.123* in HTTP user-agent header field:

```
http user-agent = xyz.123
```

http version

This command allows you to define rule expressions to match version information in HTTP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http version [case-sensitive] *operator http_version*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

http_version

Specifies this HTTP version value to match.
http_version must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

Usage

Use this command to define rule expressions to match HTTP version.

Example

The following command defines a rule expression to match HTTP version *http4.2*:

```
http version = http4.2
```

http x-header

This command allows you to define rule expressions to match specified field within extension-headers (x-headers).

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] http x-header *field_name* **[case-sensitive]** *operator string*

no

If previously configured, deletes the specified rule expression from the current ruledef.

field_name

field_name must be an alphanumeric string of 1 through 31 characters.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

string

Specifies the HTTP x-header value to match.
string must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match specified fields within x-headers. The extension-header can be any header fields which are not specified in an RFC.
All x-header fields must begin with “x-”.

Example

The following command defines a rule expression to match the extension-header *test_field* for the value *test_string*:

```
http x-header test_field = test_string
```

icmp any-match

This command allows you to define rule expressions to match all ICMP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] icmp any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all ICMP packets.

Example

The following command defines a rule expression to match all ICMP packets:

```
icmp any-match = TRUE
```

icmp code

This command allows you to define rule expressions to match value in the Code field of ICMP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] icmp code operator code
```

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

code

Specifies the ICMP code to match.
code must be an integer from 0 through 255.

Usage

Use this command to define rule expressions to match a code field of ICMP packets.

Example

The following command defines a rule expression to match ICMP code *11*:

```
icmp code = 11
```

icmp type

This command allows you to define rule expressions to match value in Type field of ICMP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] icmp type *operator type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

type

Specifies the ICMP type to match.
type must be an integer from 0 through 255. For example, 0 for Echo Reply, 3 for Destination Unreachable, and 5 for Redirect.

Usage

Use this command to define rule expressions to match a type field of ICMP packets.

Example

The following command defines a rule expression to match user traffic based on ICMP type *3*:

```
icmp type = 3
```

icmpv6 any-match

This command allows you to define rule expressions to match all ICMPv6 packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] icmpv6 any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all ICMPv6 packets.

Example

The following command defines a rule expression to match all ICMPv6 packets:

```
icmpv6 any-match = TRUE
```

icmpv6 code

This command allows you to define rule expressions to match value in Code field of ICMPv6 packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] icmpv6 code *operator code*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

code

Specifies the ICMPv6 code to match.
code must be an integer from 0 through 255.

Usage

Use this command to define rule expressions to match a code field of ICMPv6 packets.

Example

The following command defines a rule expression to match ICMPv6 code *134*:

```
icmpv6 code = 134
```

icmpv6 type

This command allows you to define rule expressions to match type field of ICMPv6 packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] icmpv6 type *operator type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

type

Specifies the ICMPv6 type to match.
type must be an integer from 0 through 255. For example, 129 for Echo Reply, 3 for Time Exceeded, and 137 for Redirect Message.

Usage

Use this command to define rule expressions to match type field of ICMPv6 packets.

Example

The following command defines a rule expression to match ICMPv6 type *133*:

```
icmpv6 type = 133
```

if-protocol

This command allows you to associate different content IDs with the same ruledef, depending on the protocol being used.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

if-protocol { http | wsp-connection-less | wsp-connection-oriented } content-id *content_id*

no if-protocol { http | wsp-connection-less | wsp-connection-oriented }

no

If previously configured, deletes the specified rule expression from the current ruledef.

http

Specifies HTTP protocol.
This is the same as the rule expression **http any-match = true**.

wsp-connection-less

Specifies WSP connection-less protocol.
This is the same as requiring "**wsp any-match = true**" but "**wtp any-match = false**" (that is, connection-less WAP1.x).

wsp-connection-oriented

Specifies WSP connection-oriented protocol.
This is the same as the combined rule expression "**wsp any-match = true**" and "**wtp any-match = true**" (that is, connection-oriented WAP1.x).

content-id *content_id*

Specifies the content ID for the specified protocol.
In 12.1 and earlier releases, *content_id* must be an integer from 1 through 65535.
In 12.2 and later releases, *content_id* must be an integer from 1 through 2147483647.

Usage

Use this command to associate different content IDs with the same ruledef, depending on the protocol being used.
This command is only effective for charging ruledefs. See the rule-application command for information on how to configure charging ruledefs.
If a particular ruledef should have three different values for content-id, depending on whether the traffic is connection-oriented WAP1.x, connection-less WAP1.x, or WAP2.0, within the ruledef we should have configuration similar to the following:

if-protocol wsp-connection-oriented content-id *1*
if-protocol wsp-connection-less content-id *2*
if-protocol http content-id *3*
Presumably, the ruledef would have another configurable like "**www url contains** *foo*", which would cause it to use different content IDs when "foo" was accessed, depending upon the protocol being used.

Example

The following command associates HTTP protocol and a content ID of *23*:

```
if-protocol http content-id 23
```

imap any-match

This command allows you to define rule expressions to match all IMAP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] imap any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all IMAP packets.

Example

The following command defines a rule expression to match all IMAP packets:

```
imap any-match = TRUE
```

imap cc

This command allows you to define rule expressions to match recipient address in the Carbon Copy (cc) field of e-mails in IMAP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] imap cc [case-sensitive] *operator cc_address*

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

---

cc_address

Specifies the e-mail "cc" address/name to match.
cc_address must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match recipient address in the "cc" field of e-mails in IMAP messages.

Example

The following command defines a rule expression to match recipient address *triangle@xyz.com* in the "cc" field of e-mails in IMAP messages:

```
imap cc contains triangle@xyz.com
```

imap command

This command allows you to define rule expressions to match embedded IMAP commands in IMAP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] imap command *operator command*

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

---

command

Specifies the command to match.
command must be one of the following:

- **append**
- **authenticate**
- **capability**
- **check**
- **close**
- **copy**
- **create**
- **delete**
- **examine**
- **expunge**
- **fetch**
- **list**
- **login**
- **logout**
- **lsub**
- **noop**
- **rename**

- **search**
- **select**
- **starttls**
- **status**
- **store**
- **subscribe**
- **uid-copy**
- **uid-fetch**
- **uid-search**
- **uid-store**
- **unsubscribe**

Usage

Use this command to define rule expressions to match an embedded command in the IMAP message.

Example

The following command defines a rule expression to match **close** command in IMAP messages:

```
imap command = close
```

imap content class

This command allows you to define rule expressions to match the content-class field of e-mails in IMAP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] imap content class [ case-sensitive ]` *`operator content_class`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`content_class`

Specifies the content class to match.
`content_class` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the content-class field of e-mails in IMAP messages.

Example

The following command defines a rule expression to analyze user traffic matching content class *`javax.mail.internet.MimeMultipart`* in the content-class field of e-mails in IMAP messages:

```
imap content class contains javax.mail.internet.MimeMultipart
```

imap content type

This command allows you to define rule expressions to match the content-type field of e-mails in IMAP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] imap content type [case-sensitive] *operator content_type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

content_type

Specifies the content type field to match.
content_type must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the content-type field of e-mails in IMAP messages.

Example

The following command defines a rule expression to analyze user traffic matching content type *TEXT/plain; charset=iso-8859-1* in the content-type field of e-mails in IMAP messages:

```
imap content type contains TEXT/plain; charset=iso-8859-1
```

imap date

This command allows you to define rule expressions to match the Date field of e-mails in IMAP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] imap date [case-sensitive] *operator date*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

date

Specifies the date to match.
date must be an alphanumeric string of 1 through 127 characters that may include punctuation marks and spaces as shown in the example below.

Usage

Use this command to define rule expressions to match the date field of e-mails in IMAP messages.

Example

The following command defines a rule expression to analyze user traffic matching date *Fri, 20 Jan 2012 11:00:00 -0600* in the “date” field of e-mails in IMAP messages:

```
imap date contains Fri, 21 Jan 2012 11:00:00 -0600
```

imap final-reply

This command allows you to define rule expressions to match final-reply value for the last IMAP final-reply message.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] imap final-reply *operator final_reply*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

final_reply

Specifies the "final-reply" condition to match.
final_reply must be one of the following:

- **bad**: Final reply is invalid or bad.
- **no**: There is no final reply.
- **ok**: Final reply is valid.

Usage

Use this command to define rule expressions to match a final-reply value for the last IMAP final-reply message.

Example

The following command defines a rule expression to analyze user traffic matching the final-reply condition **bad** in the last IMAP final-reply message:

```
imap final-reply = bad
```

imap from

This command allows you to define rule expressions to match the from field of e-mails in IMAP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] imap from [ case-sensitive ]` *`operator from_address`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`from_address`

Specifies the "from" address/value to match.
`from_address` must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match the from field of e-mails in IMAP messages.

Example

The following command defines a rule expression to analyze user traffic matching *`triangle`* in the "from" field of e-mails in the IMAP messages:

```
imap from contains triangle
```

imap mail-size

This command allows you to define rule expressions to match IMAP e-mail users that have e-mails of a specified size in their mailboxes.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] imap mail-size *operator mail_size*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

mail_size

Specifies the total size of mail, in bytes, to match.
mail_size must be an integer from 0 through 4000000000.

Usage

Use this command to define rule expressions to discover the number of IMAP e-mail users that have e-mails of a specified size in their mailboxes.

Example

The following command defines a rule expression to match users with e-mail size less than or equal to *23400* bytes:

```
imap mail-size <= 23400
```

imap mailbox-size

This command allows you to define rule expressions to match IMAP e-mail user having a specified number of messages in their mailboxes.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] imap mailbox-size *operator number_of_email*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

number_of_email

Specifies the total number of e-mail messages in mailbox of an IMAP user to match.
number_of_email must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match the number of IMAP e-mail users having a specified number of messages in their mailboxes.

Example

The following command defines a rule expression to match e-mail users having less than or equal to *1024* e-mail messages in their mailboxes:

```
imap mailbox-size <= 1024
```

imap message-type

This command allows you to define rule expressions to match the type of IMAP packet.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] imap message-type *operator message_type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

message_type

Specifies the IMAP packet message-type to match.
message_type must be one of the following:

- **command-continuation-reply**: Message with command-continuation-reply type.
- **final-reply**: Message is of final reply type.
- **request**: There is of request type.
- **untagged-reply**: Message of reply type, but without any tag.

Usage

Use this command to define rule expressions to match the IMAP message type.

Example

The following command defines a rule expression to match IMAP sessions with message type **request**:

```
imap message-type = request
```

imap previous-state

This command allows you to define rule expressions to match the previous state of IMAP request sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] imap previous-state` *`operator imap_previous_state`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`=`**: Equals

`imap_previous_state`

Specifies the previous state to match.
`imap_previous_state` must be one of the following:

- **`init`**: Message in initialization state.
- **`request-sent`**: Message in request-sent state.

Usage

Use this command to define rule expressions to match previous state of IMAP request session.

Example

The following command defines a rule expression to match IMAP sessions with previous state **`init`**:

```
imap previous-state = init
```

imap session-length

This command allows you to define rule expressions to match the total length of an IMAP session.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] imap session-length *operator session_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

session_length

Specifies the total length of IMAP session (in bytes) to match.
session_length must be an integer from 1 through 4000000000.

Usage

Use this command to define rule expressions to match the total length of IMAP sessions.
The session length is calculated by adding together the IP payloads (that is, starting after the IP header) of all relevant IMAP session packets.

Example

The following command defines a rule expression to match IMAP sessions with length less than or equal to *4000* bytes:

```
imap session-length <= 4000
```

imap session-previous-state

This command allows you to define rule expressions to match the previous state of an IMAP session.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] imap session-previous-state *operator imap_session_previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

imap_session_previous_state

Specifies the previous state of IMAP session to match.
imap_session_previous_state must be one of the following:

- **authenticated**: Session authenticated
- **connected**: Session connected
- **init**: Session initialized
- **mailbox-selected**: Mailbox selected

Usage

Use this command to define rule expressions to match the previous state of IMAP sessions.

Example

The following command defines a rule expression to match IMAP sessions with previous state **init**:

```
imap session-previous-state = init
```

imap session-state

This command allows you to define rule expressions to match the current state of IMAP sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] imap session-state *operator session_current_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

session_current_state

Specifies the current state to match.
session_current_state must be one of the following:

- **authenticated**: Session authenticating.
- **connected**: Session connecting.
- **logout**: Session logged out.
- **mailbox-selected**: Mailbox selecting.

Usage

Use this command to define rule expressions to match the current state of IMAP sessions.

Example

The following command defines a rule expression to match IMAP sessions with current state **connected**:

```
imap session-state = connected
```

imap state

This command allows you to define rule expressions to match the current state of IMAP sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] imap state *operator current_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

current_state

Specifies current state of IMAP session to match.
current_state must be one of the following:

- **request-sent**: Request message sent
- **response-fail**: Request response failed
- **response-ok**: Request response is good

Usage

Use this command to define rule expressions to match the current state of IMAP session.

Example

The following command defines a rule expression to match IMAP sessions with current state **response-fail**:

```
imap state = response-fail
```

imap subject

This command allows you to define rule expressions to match the subject field of e-mails in IMAP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] imap subject [case-sensitive] *operator subject*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

subject

Specifies the "subject" to match.
subject must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters and space as shown in the example below.

Usage

Use this command to define rule expressions to match "subject" field of e-mail in IMAP message.

Example

The following command defines rule expression to match occurrence of the string *My test* in the "subject" field of e-mails in IMAP message:

```
imap subject contains My test
```

imap to

This command allows you to define rule expressions to match the “to” field of e-mails in IMAP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] imap to [ case-sensitive ]` *`operator to`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`to`

Specifies the “to” field value to match.
`to` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match “to” field of e-mails in IMAP messages.

Example

The following command defines a rule expression to analyze user traffic matching the occurrence *`xyz.com`* in the “to” field of e-mails in the IMAP message:

```
imap to contains xyz.com
```

ip any-match

This command allows you to define rule expressions to match all IPv4/IPv6 packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ip any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match IPv4/IPv6 packets.

Example

The following command defines a rule expression to match IPv4/IPv6 packets:

```
ip any-match = TRUE
```

ip downlink

This command allows you to define rule expressions to match downlink (network to subscriber) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ip downlink *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match downlink (to subscriber) IP packets.

Example

The following command defines a rule expression to match IP packet in downlink direction:

```
ip downlink = TRUE
```

ip dst-address

This command allows you to define rule expressions to match IP destination address field within IP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ip dst-address { *operator* { *ip_address* | *ip_address/mask* } | { !range | range } host-pool *host_pool_name* }

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator **{** *ip_address* **|** *ip_address/mask* **}**

operator: Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

ip_address: Specifies the IP address of the destination node for outgoing traffic. *ip_address* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.
ip_address/mask: Specifies the IP address of the destination node for outgoing traffic. *ip_address/mask* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated notation with subnet mask bit. The mask bit is a numeric value which corresponding to the number of bits in the subnet mask.

{ !range | range } host-pool *host_pool_name*

!range | range: Specifies the range criteria:

- **!range**: Not in the range of
- **range**: In the range of

host-pool *host_pool_name*: Specifies the name of the host pool. *host_pool_name* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define rule expressions to match the IP destination address field within IP headers.

Example

The following command defines a rule expression to match the IPv4 destination address *10.1.1.1*:

```
ip dst-address = 10.1.1.1
```

ip error

This command allows you to define rule expressions to match user traffic for invalid IP packets and other errors, for example IP header error, while parsing IP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ip error *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match invalid IP packets and any other errors while parsing IP packets.

Example

The following command defines a rule expression to match user traffic for invalid IP packets and other errors:

```
ip error = TRUE
```

ip protocol

This command allows you to define rule expressions to match the protocol field in IP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ip protocol *operator* **{** *protocol_assignment_no* **|** *protocol* **}**

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals—available only in 8.1 and later releases
- **=**: Equals
- **>=**: Greater than or equals—available only in 8.1 and later releases

protocol_assignment_no

Specifies the protocol by assignment number.
protocol_assignment_no must be an integer from 0 through 255.
For example, 1 for ICMP, 6 for TCP, and 17 for UDP.

protocol

Specifies the protocol by name.
protocol must be one of the following:

- **ah**
- **esp**
- **gre**
- **icmp**
- **icmpv6**
- **tcp**
- **udp**

Usage

Use this command to define rule expressions to match protocol field in IP packet headers.

Example

The following command defines a rule expression to match protocol assignment number *1*:

```
ip protocol = 1
```

ip server-domain-name

This command allows you to define rule expressions to match host names (domain names).

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ip server-domain-name *operator domain_name*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

domain_name

Specifies the domain name to match.
domain_name must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match full or partial host names (domain names).
The rule will be matched for the learnt IP addresses resolved from DNS queries to the specified domain names. DNS responses for the specified domain names will be snooped and the learnt IP addresses stored. Besides being used for standard rule matching, this command also enables the DNS Snooping feature if the rulebase references any ruledefs with this configuration. The DNS protocol analyzer must also be enabled in the rulebase.

Example

The following command defines a rule expression to match domain name values containing *star*:

```
ip server-domain-name contains star
```

ip server-ip-address

This command allows you to define rule expressions to match the IP address of the destination end of the connection.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ip server-ip-address { *operator* **{** *ip_address* **|** *ip_address/mask* **} | { !range | range } host-pool** *host_pool_name* **}**

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator **{** *ip_address* **|** *ip_address/mask* **}**

operator: Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

ip_address: Specifies the server IP address. For uplink packets (subscriber to network), this field matches the destination IP address in the IP header. For downlink packets (network to subscriber), this field matches the source IP address in the IP header.*ip_address* must be an IP address in IPv4 dotted-decimal notation or IPv6 colon-separated notation.
ip_address/mask: Specifies the server IP address with subnet mask bit. For uplink packets (subscriber to network), this field matches the destination IP address in the IP header. For downlink packets (network to subscriber), this field matches the source IP address in the IP header. *ip_address/mask* must be an IP address in IPv4 dotted-decimal notation or IPv6 colon-separated notation with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.

{ !range | range } host-pool *host_pool_name*

!range | range: Specifies the range criteria:

- **!range**: Not in the range of
- **range**: In the range of

host-pool *host_pool_name*: Specifies name of the host pool. *host_pool_name* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define rule expressions to match the IP address of the destination end of the connection. For uplink packets, this field matches the destination IP address in the IP header. For downlink packets, this field matches the source IP address in the IP header.

Example

The following command defines a rule expression to match user traffic based on IPv4 server address *10.1.1.1*:

```
ip server-ip-address = 10.1.1.1
```

ip src-address

This command allows you to define rule expressions to match the source IP address field within IP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ip src-address { *operator* **{** *ip_address* **|** *ip_address/mask* **} | { !range | range }**
host-pool *host_pool_name* **}**

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator **{** *ip_address* **|** *ip_address/mask* **}**

operator: Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

ip_address: Specifies IP address of the source node for incoming traffic. *ip_address* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.
ip_address/mask: Specifies the IP address of the source node for incoming traffic with subnet mask bit. *ip_address/mask* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated notation with subnet mask bit. The mask bit is a numeric value which corresponds to the number of bits in the subnet mask.

{ !range | range } host-pool *host_pool_name*

!range | range: Specifies the range criteria:

- **!range**: Not in the range of
- **range**: In the range of

host-pool *host_pool_name*: Specifies name of the host pool. *host_pool_name* must be a string of 1 through 63 characters.

Usage

Use this command to define rule expressions to match IP source address field within IP header.

Example

The following command defines a rule expression to match user traffic based on IPv4 source address *10.1.1.1*:

```
ip src-address = 10.1.1.1
```

ip subscriber-ip-address

This command allows you to define rule expressions to match the IP address of the subscriber, which will be either the source or destination address depending on the direction.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ip subscriber-ip-address { *operator* **{** *ip_address* **|** *ip_address/mask* **} | { !range | range } host-pool** *host_pool_name* **}**

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator **{** *ip_address* **|** *ip_address/mask* **}**

operator: Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

ip_address: Specifies the subscriber IP address. Depending on the direction of packet this IP address will be either the IP source address or the IP destination address. *ip_address* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.
ip_address/mask: Specifies the subscriber IP address with subnet mask bit. Depending on the direction of packet this IP address will either be the IP source address or the IP destination address. *ip_address/mask* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated notation with subnet mask bit. The mask bit is a numeric value which corresponds to the number of bits in the subnet mask.

{ !range | range } host-pool *host_pool_name*

!range | range: Specifies the range criteria:

- **!range**: Not in the range of
- **range**: In the range of

host-pool *host_pool_name*: Specifies the name of the host pool. *host_pool_name* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define rule expressions to match the IP address of the subscriber, which will be either the source or destination address depending on the direction.

Example

The following command defines a rule expression to match user traffic based on subscriber IPv4 address *10.1.1.1*:

```
ip subscriber-ip-address = 10.1.1.1
```

ip total-length

This command allows you to define rule expressions to match the total length field in IP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ip total-length *operator total_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

total_length

Specifies the total length of the IP packet (including payload) to match.
total_length must be an integer from 0 through 4096.

Usage

Use this command to define rule expressions to match the total length field in IP headers.

Example

The following command defines a rule expression to match user traffic based on IP total length of *2000* bytes:

```
ip total-length = 2000
```

ip uplink

This command allows you to define rule expressions to match uplink (subscriber to network) IP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] ip uplink` *`operator condition`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`=`**: Equals

`condition`

Specifies the condition to match.
`condition` must be one of the following:

- **`FALSE`**
- **`TRUE`**

Usage

Use this command to define rule expressions to match uplink (subscriber to network) IP packets.

Example

The following command defines a rule expression to match uplink packets:

```
ip uplink = TRUE
```

ip version

This command allows you to define rule expressions to match the version number in IP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] ip version *operator ip_version*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be **=** (equals).

ip_version

Specifies the IP version to match.
ip_version must be one of the following:

- **ipv4**
- **ipv6**

Usage

Use this command to define rule expressions to match version number in IP header.

Example

The following command defines a rule expression to match user traffic for the IP version **ipv6**:

```
ip version = ipv6
```

mms any-match

This command allows you to define rule expressions to match all Multimedia Messenging Service (MMS) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all MMS packets.

Example

The following command defines a rule expression to match all MMS packets:

```
mms any-match = TRUE
```

mms bcc

This command allows you to define rule expressions to match recipient addresses in the bcc field of MMS messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] mms bcc [ case-sensitive ]` *`operator bcc_address`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`bcc_address`

Specifies the “bcc” address/value to match.
`bcc_address` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.

Usage

Use this command to define rule expressions to match recipient address in the “bcc” field of MMS messages.

Example

The following command defines a rule expression to match recipient address containing *`test1`* in “bcc” field of MMS messages:

```
mms bcc contains test1
```

mms cc

This command allows you to define rule expressions to match recipient addresses in the cc field of MMS messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] mms cc [ case-sensitive ]` *`operator cc_address`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`cc_address`

Specifies the "cc" address/value to match.
`cc_address` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.

Usage

Use this command to define rule expressions to match recipient addresses in "cc" field of MMS messages.

Example

The following command defines a rule expression to match recipient address containing *`test1`* in the "cc" field of MMS messages:

```
mms cc contains test1
```

mms content location

This command allows you to define rule expressions to match the content-location field of MMS messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms content location [case-sensitive] *operator string*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

string

Specifies the value to match.
string must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.

Usage

Use this command to define rule expressions to match the content-location field of MMS messages.

Example

The following command defines a rule expression to match *test1* in content-location field of MMS messages:

```
mms content location contains test1
```

mms content type

This command allows you to define rule expressions to match the content-type field of MMS messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms content type [case-sensitive] *operator content_type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

content_type

Specifies the MMS content type to match.
content_type must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.

Usage

Use this command to define rule expressions to match content-type field of MMS messages.

Example

The following command defines a rule expression to match *image* in content-type field of MMS messages:

```
mms content type contains image
```

mms downlink

This command allows you to define rule expressions to match downlink (network to subscriber) MMS packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms downlink *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the downlink (from the Mobile Node direction) status to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match downlink MMS packets.

Example

The following command defines a rule expression to match all downlink MMS packets:

```
mms downlink = TRUE
```

mms from

This command allows you to define rule expressions to match the “from” field in MMS messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms from [case-sensitive] *operator from_address*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

from_address

Specifies the “from” address/value to match.
from_address must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.

Usage

Use this command to define rule expressions to match the “from” field of MMS messages.

Example

The following command defines a rule expression to match *test1* in the “from” field of MMS messages:

```
mms from contains test1
```

mms message-id

This command allows you to define rule expressions to match the message ID field of MMS messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms message-id [case-sensitive] *operator message_id*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

message_id

Specifies the MMS message ID to match.
message_id must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the “message ID” field of MMS messages.

Example

The following command defines a rule expression to match *test1* in the “message ID” field of MMS messages:

```
mms message-id contains test1
```

mms pdu-type

This command allows you to define rule expressions to match Protocol Data Unit (PDU) type in the current MMS packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms pdu-type *operator pdu_type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

pdu_type

Specifies the MMS PDU type to match.
pdu_type must be one of the following:

- **mms-pdu-type-m-acknowledge-ind**
- **mms-pdu-type-m-delivery-ind**
- **mms-pdu-type-m-http-get**
- **mms-pdu-type-m-notification-ind**
- **mms-pdu-type-m-notify-rsp-ind**
- **mms-pdu-type-m-retrieve-conf**
- **mms-pdu-type-m-send-conf**
- **mms-pdu-type-m-send-request**
- **mms-pdu-type-m-wsp-get**
- **mms-pdu-type-response**: This option is deprecated. Use the **mms_pdu_type_m_retrieve_conf** option instead.

Usage

Use this command to define rule expressions to match the PDU type in the current MMS packet.

Example

The following command defines a rule expression to match PDU type **mms-pdu-type-m-http-get** in the current MMS packet:

```
mms pdu-type = mms-pdu-type-m-http-get
```

mms previous-state

This command allows you to define rule expressions to match the previous state of MMS sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms previous-state *operator mss_previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

mms_previous_state

Specifies the previous state to match.
mms_previous_state must be one of the following:

- **delayed-ack-pending**: This option is deprecated, use **retrieve-conf-received**.
- **delayed-m-notify-rsp-sent**: This option is deprecated, use **notify-rsp-sent**.
- **delayed-retrieval-pending**: This option is deprecated, use **retrieval-pending**.
- **immediate-retrieval-pending**: This option is deprecated, use **retrieval-pending**.
- **init**
- **m-send-conf-rcvd**: This option is deprecated, use **send-success**.
- **m-send-req-sent**
- **notification-ind-rcvd**
- **notify-rsp-sent**
- **retrieval-pending**
- **retrieve-conf-received**
- **send-success**

Usage

Use this command to define rule expressions to match the previous state of MMS sessions.

Example

The following command defines a rule expression to match user traffic based on MMS previous state of **retrieval-pending**:

```
mms previous-state = retrieval-pending
```

mms response status

This command allows you to define rule expressions to match the response status code of MMS messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms response status *operator status_code*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

status_code

Specifies the status code to match.
status_code must be an integer from 128 through 136.

Usage

Use this command to define rule expressions to match response status code of MMS messages.

Example

The following command defines a rule expression to match user traffic based on MMS response status code *129*:

```
mms response status = 129
```

mms state

This command allows you to define rule expressions to match the current state of MMS sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms state *operator current_state*

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

---

current_state

Specifies current state of MMS session to match.
current_state must be one of the following:

- **delayed-ack-pending**: This option is deprecated, use **retrieve-conf-received**.
- **delayed-m-notify-rsp-sent**: This option is deprecated, use **notify-rsp-sent**.
- **delayed-retrieval-pending**: This option is deprecated, use **retrieval-pending**.
- **delivery-failed**
- **delivery-success**
- **immediate-retrieval-pending**: This option is deprecated, use **retrieval-pending**.
- **m-send-conf-rcvd**: This option is deprecated, use **send-success**.
- **m-send-req-sent**
- **notification-ind-rcvd**
- **notify-rsp-sent**
- **retrieval-failed**
- **retrieval-pending**
- **retrieval-success**
- **retrieve-conf-received**
- **send-success**

Usage

Use this command to define rule expressions to match the current state of MMS session.

Example

The following command defines a rule expression to match user traffic based on the current state of MMS session as **retrieval-failed**:

```
mms state = retrieval-failed
```

mms status

This command allows you to define rule expressions to match the current status of MMS sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms status *operator status*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

status

Specifies the MMS status to match.
status must be an integer from 128 through 132.

Usage

Use this command to define rule expressions to match current status of MMS sessions.

Example

The following command defines a rule expression to match user traffic based on MMS current status *130*:

```
mms status = 130
```

mms subject

This command allows you to define rule expressions to match the “subject” field of MMS messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms subject [case-sensitive] *operator subject_string*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

subject_string

Specifies the value to match.
subject_string must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.

Usage

Use this command to define rule expressions to match “subject” field of MMS messages.

Example

The following command defines a rule expression to match *test1* in the “subject” field of MMS messages:

```
mms subject contains test1
```

mms tid

This command allows you to define rule expressions to match the "Transaction Identifier" (TID) field of MMS messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms tid [case-sensitive] *operator transaction_id*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

transaction_id

Specifies the MMS TID to match.
transaction_id must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match TID field of MMS messages.

Example

The following command defines a rule expression to match *test* in TID field of MMS messages:

```
mms tid = test
```

mms to

This command allows you to define rule expressions to match the “to” field of MMS messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms to [case-sensitive] *operator to_address*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

to_address

Specifies the “to” address/name to match.
to_address must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters and space.

Usage

Use this command to define rule expressions to match “to” field of MMS messages.

Example

The following command defines a rule expression to match user traffic based on *test* in “to” field of MMS messages:

```
mms to = test
```

mms uplink

This command allows you to define rule expressions to match uplink (subscriber to network) MMS packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms uplink *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the uplink (from the Mobile Node direction) status to match.
condition must one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match uplink MMS packets.

Example

The following command defines a rule expression to match uplink MMS packets:

```
mms uplink = TRUE
```

mms version

This command allows you to define rule expressions to match the MMS version in MMS packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] mms version *operator version*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

version

Specifies the MMS version to match.
version must be an integer from 1 through 65535.

Important: MMS protocol analyzer supports decoding of only MMS version 1.0.

Usage

Use this command to define rule expressions to match MMS version in MMS packets.

Example

The following command defines a rule expression to match MMS version *1.0* in MMS packets:

```
mms version = 1
```

multi-line-or all-lines

This command applies the OR operator to all lines in the current ruledef.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] multi-line-or all-lines
```

no

If previously configured, deletes this configuration in the current ruledef.

multi-line-or all-lines

Applies the OR operator to all lines in the current ruledef.

Usage

When a ruledef is evaluated, if the **multi-line-or all-lines** command is configured, the logical OR operator is applied to all the rule expressions in the ruledef to decide if the ruledef matches or not. If the **multi-line-or all-lines** command is not configured, the logical AND operator is applied to all the rule expressions.

The intent of this command is to allow a single ruledef to specify multiple URL expressions. Otherwise, multiple ruledefs need to be created, each with one URL expression. When this CLI command is used, each expression in the ruledef impacts the total number of ruledefs allowed. So from a “maximum number of possible ruledefs” perspective, it makes no difference whether there are N ruledefs with one expression each, or one ruledef with N expressions.

p2p any-match

This command allows you to define rule expressions to match all Peer-to-Peer (P2P) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] p2p any-match` *`operator condition`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`=`**: Equals

`condition`

Specifies the condition to match.
`condition` must be one of the following:

- **`TRUE`**: The rule matches any P2P traffic.
- **`FALSE`**: The rule does not match any P2P traffic.

Usage

Use this command to define rule expressions to match all P2P packets.

Example

The following command defines a rule expression to match all P2P packets:

```
p2p any-match = TRUE
```

p2p protocol

This command allows you to define rule expressions to match P2P protocol. This command must be used for charging purposes. It must not be used for detection purposes.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] p2p protocol *operator protocol*

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.
operator must be **=** (equals).

---

protocol

Specifies the protocol to match.
protocol must be one of the following:

- **actsync**
- **aimini**
- **antsp2p**
- **applejuice**
- **ares**
- **armagettron**
- **battlefld**
- **bittorrent**
- **blackberry**
- **citrix**
- **clubpenguin**
- **crossfire**
- **ddlink**
- **directconnect**
- **dofus**
- **edonkey**
- **facebook**
- **facetime**

Important: The **facetime** protocol is available only in 9.0 and in 11.0 and later releases.

- **fasttrack**
- **feidian**
- **fiesta**
- **filetopia**
- **florensia**
- **freenet**
- **fring**
- **funshion**
- **gadugadu**
- **gamekit**

Important: The **gamekit** protocol is available only in 9.0 and in 11.0 and later releases.

- **gmail**
- **gnutella**
- **gtalk**
- **guildwars**
- **halflife2**
- **hamachivpn**
- **iax**
- **icecast**
- **imesh**
- **imo**
- **iptv**
- **irc**
- **isakmp**
- **iskoot**
- **itunes**
- **jabber**
- **kontiki**
- **manolito**
- **maplestory**
- **meebo**
- **mgcp**

- msn
- mute
- mypeople
- myspace
- netmotion
- nimbuzz
- octoshape
- off
- ogg
- oovoo
- openft
- openvpn
- orb
- oscar
- paltalk
- pando
- pandora
- popo
- pplive
- ppstream
- ps3
- qq
- qqgame
- qqlive
- quake
- quicktime
- rdp
- rdt
- rfactor
- rmstream
- scydo
- secondlife
- shoutcast
- skinny
- skype
- slingbox
- sopcast

- **soulseek**
- **splashfighter**
- **spotify**
- **ssdp**
- **stealthnet**
- **steam**
- **stun**
- **tango**
- **teamspeak**
- **teamviewer**
- **thunder**
- **tor**
- **truphone**
- **tunnelvoice**
- **tvants**
- **tvuplayer**
- **twitter**
- **ultrabac**
- **usenet**
- **uusee**
- **veohtv**
- **viber**
- **vpnx**
- **vtun**
- **warcft3**
- **whatsapp**
- **wii**
- **winmx**
- **winny**
- **wmstream**
- **wofkungfu**
- **wofwarcraft**
- **xbox**
- **xdcc**
- **yahoo**
- **yourfreetunnel**
- **zattoo**

Usage

Use this command to define rule expressions to detect P2P protocols for charging purposes. For detection purposes use the **p2p-detection protocol** command in the ACS Configuration Mode.

Example

The following command specifies to detect orb protocol for charging purposes:

```
p2p protocol = orb
```

p2p traffic-type

This command allows you to define rule expressions to match traffic type—audio, video, and unclassified.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] p2p traffic-type *operator traffic_type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

traffic_type

Specifies the traffic type to match.
In 11.0 and later releases, *traffic_type* must be one of the following:

- **audio**
- **unclassified**
- **video**

In 10.0 and earlier releases, *traffic_type* must be **voice**.

Usage

Use this command to configure the system to detect voice or non-voice P2P traffic. When the detection of a protocol is enabled then the detection of sub-type is enabled by default.

Example

The following command configures the system to detect video traffic:

```
p2p traffic-type = video
```

pop3 any-match

This command allows you to define rule expressions to match all Post Office Protocol 3 (POP3) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pop3 any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all POP3 packets.

Example

The following command defines a rule expression to match all POP3 packets:

```
pop3 any-match = TRUE
```

pop3 command args

This command allows you to define rule expressions to match POP3 command arguments.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] pop3 command args [ case-sensitive ]` *`operator argument`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`argument`

Specifies the command argument to match.
`argument` must be an alphanumeric string of 1 through 40 characters, and may contain punctuation characters.

Usage

Use this command to define rule expressions to match POP3 command argument.

Example

The following command defines a rule expression to match POP3 command argument *`test`*:

```
pop3 command args = test
```

pop3 command id

This command allows you to define rule expressions to match POP3 command ID.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pop3 command id *operator command_id*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

command_id

Specifies the command ID to match.
command_id must be an integer from 1 through 12.

Usage

Use this command to define rule expressions to match a POP3 command ID.

Example

The following command defines a rule expression to match POP3 command ID *8*:

```
pop3 command id = 8
```

pop3 command name

This command allows you to define rule expressions to match command sent within a POP3 packet.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pop3 command name *operator command_name*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

command_name

Specifies the command name to match.
command_name must be one of the following:

- **apop**
- **dele**
- **list**
- **noop**
- **pass**
- **quit**
- **retr**
- **reset**
- **stat**
- **top**
- **uidl**
- **user**

Usage

Use this command to define rule expressions to match commands sent within POP3 packets.

Example

The following command defines a rule expression to match the **list** command sent in POP3 packets:

```
pop3 command name = list
```

pop3 mail-size

This command allows you to define rule expressions to match POP3 mail size.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pop3 mail-size { *operator mail_size* **| { range | !range }** *range_from* **to** *range_to* **}**

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

{ range | !range } *range_from* **to** *range_to*

Enables or disables the range criteria.

- **range**: Enables the range criteria.
- **!range**: Disables the range criteria.
- *range_from*: Specifies start of the range.

  range_from must be an integer from 1 through 4000000000.
- *range_to*: Specifies the end range.

  range_to must be an integer from 1 through 4000000000, and must be greater than *range_from*.

mail_size

Specifies the mail size to match.
mail_size must be an integer from 1 through 4000000000.

Usage

Use this command to define rule expressions to match POP3 mail size.

Example

The following command defines a rule expression to match POP3 mail size of *40000*:

```
pop3 mail-size = 40000
```

pop3 pdu-length

This command allows you to define rule expressions to match the Protocol Data Unit (PDU) length of POP3 packets equal to the POP3 header plus POP3 payload.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pop3 pdu-length { *operator pdu_length* **| { { range | !range }** *range_from* **to** *range_to* **} }**

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

{ range | !range } *range_from* **to** *range_to*

Enables or disables the range criteria.

- **range**: Enables the range criteria.
- **!range**: Disables the range criteria.
- *range_from*: Specifies the start of range as an integer from 0 through 65535.
- *range_to*: Specifies the end range. *range_to* must be an integer from 0 through 65535, and must be greater than *range_from*.

pdu_length

Specifies the POP3 PDU length to match.
pdu_length must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match POP3 PDU length (header + payload) in bytes.

Example

The following command defines a rule expression to match PDU length of *1000* bytes:

```
pop3 pdu-length = 1000
```

pop3 pdu-type

This command allows you to define rule expressions to match POP3 Protocol Data Unit (PDU) type.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pop3 pdu-type *operator pdu_type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

pdu_type

Specifies the POP3 PDU type to match.
pdu_type must be one of the following:

- **command-packet**
- **data-packet**
- **relay-packet**

Usage

Use this command to define rule expressions to match POP3 PDU type.

Example

The following command defines a rule expression to match POP3 PDU type **relay-packet**:

```
pop3 pdu-type = relay-packet
```

pop3 previous-state

This command allows you to define rule expressions to match the previous state of POP3 sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pop3 previous-state *operator pop3_previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

pop3_previous_state

Specifies the previous state to match.
pop3_previous_state must be one of the following:

- **connected**: Connected state
- **data transaction**: Data transaction state
- **init**: Initialized state
- **reply-error**: Reply error state
- **reply-ok**: Response ok state
- **waiting-for-reply**: Waiting for reply state

Usage

Use this command to define rule expressions to match a POP3 previous state.

Example

The following command defines a rule expression to match user traffic for a POP3 previous state of **connected**:

```
pop3 previous-state = connected
```

pop3 reply args

This command allows you to define rule expressions to match specified arguments with POP3 reply.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] pop3 reply args [ case-sensitive ]` *`operator argument`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`argument`

Specifies the reply argument to match.
In 11.0 and earlier releases, *`argument`* must be an alphanumeric string of 1 through 512 characters, and may contain punctuation characters.
In 12.0 and later releases, *`argument`* must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

Usage

Use this command to define rule expressions to match specified arguments within a POP3 reply.

Example

The following command defines a rule expression to match the argument *`test`* with POP3 replies:

```
pop3 reply args = test
```

pop3 reply id

This command allows you to define rule expressions to match POP3 reply ID.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pop3 reply id *operator reply_id*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

reply_id

Specifies the POP3 reply ID to match.
reply_id must be one of the following:

- **0**: Unknown reply
- **1**: +OK
- **2**: -Error

Usage

Use this command to define rule expressions to match POP3 reply ID.

Example

The following command defines a rule expression to match POP3 reply ID of *2*:

```
pop3 reply id = 2
```

pop3 reply status

This command allows you to define rule expressions to match POP3 reply status.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pop3 reply status *operator reply_status*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

reply_status

Specifies the reply status to match.
reply_status must be one of the following:

- **+OK**: Reply OK
- **-ERR**: Reply error

Usage

Use this command to define rule expressions to match POP3 reply status.

Example

The following command defines a rule expression to match POP3 reply status **+OK**:

```
pop3 reply status = +OK
```

pop3 session-length

This command allows you to define rule expressions to match POP3 session-length.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pop3 session-length { *operator session_length* **| { range | !range }** *range_from* **to** *range_to* **}**

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

session_length

Specifies the POP3 session length to match.
session_length must be an integer from 1 through 4000000000.

{ range | !range } *range_from* **to** *range_to*

Enables or disables the range criteria for PoP3 session length.

- **range**: Enables the range criteria for POP3 session length.
- **!range**: Disables the range criteria for POP3 session length.
- *range_from*: Specifies the start of range of POP3 session as an integer from 1 through 4000000000, but less than or equal to *range_to*.
- *range_to*: Specifies the end of range of POP3 session as an integer from 1 through 4000000000, but greater than or equal to *range_from*.

Usage

Use this command to define rule expressions to match the total length of POP3 sessions.

Example

The following command defines a rule expression to match a POP3 session length of *40000*:

```
pop3 session-length = 40000
```

pop3 state

This command allows you to define rule expressions to match the current state of POP3 sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pop3 state *operator current_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

current_state

Specifies the current state to match.
current_state must be one of the following:

- **close**
- **connected**
- **data-transaction**
- **reply-error**
- **reply-ok**
- **waiting-for-reply**

Usage

Use this command to define rule expressions to match the current state of POP3 sessions.

Example

The following command defines a rule expression to match the POP3 current state **close**:

```
pop3 state = close
```

pop3 user-name

This command allows you to define rule expressions to match POP3 user name.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pop3 user-name [case-sensitive] *operator user_name*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

user_name

Specifies the POP3 user name to match.
user_name must be an alphanumeric string of 1 through 64 characters, and may contain punctuation characters and space.

Usage

Use this command to define rule expressions to match POP3 user name.

Example

The following command defines a rule expression to match POP3 user name *test*:

```
pop3 user-name = test
```

pptp any-match

This command allows you to defines a rule expression to match all Point-to-Point Tunneling Protocol (PPTP) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pptp any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to specify a ruledef to analyze user traffic based on the PPTP any match status.

Example

The following command creates a PPTP ruledef for analyzing user traffic using a PPTP any match status of *FALSE*:

```
pptp any-match = FALSE
```

pptp ctrl-msg-type

This command allows you to define rule expressions to match control message type in PPTP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pptp ctrl-msg-type = *message_type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

message_type

message_type must be one of the following:

- **call-clear-request**
- **call-disconnect-notify**
- **echo-reply**
- **echo-request**
- **incoming-call-connected**
- **incoming-call-reply**
- **incoming-call-request**
- **outgoing-call-reply**
- **outgoing-call-request**
- **set-link-info**
- **start-control-connection-reply**
- **start-control-connection-request**
- **stop-control-connection-reply**
- **stop-control-connection-request**
- **wan-error-notify**

Usage

Use this command to define rule expressions to match the control message type in PPTP packets.

Example

The following command specifies to match **echo-reply** message type:

```
pptp ctrl-msg-type = echo-reply
```

pptp gre any-match

This command allows you to define rule expressions to match all PPTP Generic Routing Encapsulation (GRE) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] pptp gre any-match = *condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

condition

condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all PPTP GRE packets.

Example

The following command defines a rule expression to match all PPTP GRE packets:

```
pptp gre any-match = TRUE
```

rtcp any-match

This command allows you to define rule expressions to match all Real-Time Transport Control Protocol (RTCP) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtcp any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **TRUE**: The rule matches any RTCP traffic.
- **FALSE**: The rule does not match any RTCP traffic.

Usage

Use this command to define rule expressions to match all RTCP packets.

Example

The following command defines a rule expression to match all RTCP packets:

```
rtcp any-match = TRUE
```

rtcp jitter

This command allows you to define rule expressions to match the jitter parameter in RTCP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtcp jitter *operator jitter*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

jitter

Specifies the RTCP inter-arrival jitter value (in milliseconds) to match.
jitter must be an integer from 0 through 4294967295.

Usage

Use this command to define rule expressions to match jitter parameter found in the RTCP sender report or receiver report packets.

Example

The following command matches packets for jitter greater than or equal to 1295 milliseconds:

```
rtcp jitter >= 1295
```

rtcp parent-proto

This command allows you to define rule expressions to match the parent protocol of the RTCP flow.

Important: This command is available only in 8.1 and 9.0 and later releases.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] rtcp parent-proto` *`operator parent_protocol`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`=`**: Equals

`parent_protocol`

Specifies the RTCP parent protocol to match.
`parent_protocol` must be one of the following:

- **`rtsp`**: Real Time Streaming Protocol
- **`sip`**: Session Initiation Protocol

Usage

Use this command to define rule expressions to match user traffic based on the parent protocol of the RTCP flow.

Example

The following command defines a rule expression to match user traffic based on SIP being the parent protocol of the RTCP flow:

```
rtcp parent-proto = sip
```

rtcp pdu-length

This command allows you to define rule expressions to match Protocol Data Unit (PDU) length of RTCP packets, (RTCP header + RTCP payload).

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtcp pdu-length *operator pdu_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

pdu_length

Specifies the RTCP length (in bytes) to match.
In 8.1 and later releases, *pdu_length* must be an integer from 1 through 65535.
In 8.0, *pdu_length* must be an integer from 1 through 2000.

Usage

Use this command to define rule expressions to match RTCP PDU length (header + payload) in bytes.

Example

The following command defines a rule expression to match user traffic based on an RTCP PDU length of *10000* bytes:

```
rtcp pdu-length = 10000
```

rtcp rtsp-id

This command allows you to define rule expressions to match user traffic based on a Real-time Streaming Protocol (RTSP) ID associated with an RTCP flow.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtcp rtsp-id [case-sensitive] *operator rtsp_id*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

rtsp_id

Specifies the value to match.
rtsp_id must be an alphanumeric string of 1 through 32 characters.

Usage

Use this command to define rule expressions to match an RTSP ID associated with an RTCP flow.

Example

The following command defines a rule expression to match user traffic containing RTSP message ID of *test1*:

```
rtcp rtsp-id contains test1
```

rtcp session-length

This command allows you to define rule expressions to match the total length of RTCP sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtcp session-length *operator session_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

session_length

Specifies the RTCP total session length (in bytes) to match.
In 8.1 and later releases, *session_length* must be an integer from 1 through 4000000000.
In 8.0, *session_length* must be an integer from 1 through 40000000.

Usage

Use this command to define rule expressions to match RTCP total session length.

Example

The following command defines a rule expression to match user traffic for a total RTCP session length of *200000*:

```
rtcp session-length = 200000
```

rtcp uri

This command allows you to define rule expressions to match URI associated with RTCP flows.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtcp uri [case-sensitive] *operator uri*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

uri

Specifies the URI to match.
uri must be an alphanumeric string of 1 through 127 characters and may include punctuation characters.

Usage

Use this command to define rule expressions to match URI associated with RTCP flow.

Example

The following command defines a rule expression to match user traffic for RTCP URI *rtsp://www.example.org*:

```
rtcp uri = rtsp://www.example.org
```

rtp any-match

This command allows you to define rule expressions to match all Real-time Transport Protocol (RTP) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtp any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all RTP packets.

Example

The following command defines a rule expression to match all RTP packets:

```
rtp any-match = TRUE
```

rtp parent-proto

This command allows you to define rule expressions to match the parent protocol of the RTP flow.

Important: This command is available only in 8.1 and in 9.0 and later releases.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] rtp parent-proto` *`operator parent_protocol`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`=`**: Equals

`parent_protocol`

Specifies the RTP parent protocol to match.
`parent_protocol` must be one of the following:

- **`rtsp`**: Real Time Streaming Protocol
- **`sip`**: Session Initiation Protocol

Usage

Use this command to define rule expressions to match user traffic based on the parent protocol of the RTP flow.

Example

The following command defines a rule expression to match user traffic with parent protocol of the RTP flow being SIP:

```
rtp parent-proto = sip
```

rtp pdu-length

This command allows you to define rule expressions to match PDU length of RTP packets, equal to the RTP header + RTP payload.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtp pdu-length *operator pdu_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

pdu_length

Specifies the RTP PDU length (in bytes) to match.
In 8.1 and later releases, *pdu_length* must be an integer from 1 through 65535.
In 8.0, *pdu_length* must be an integer from 1 through 2000.

Usage

Use this command to define rule expressions to match PDU length (header + payload) of RTP packets in bytes.

Example

The following command defines a rule expression to match an RTP PDU length of *1000* bytes:

```
rtp pdu-length = 1000
```

rtp rtsp-id

This command allows you to define rule expressions to match RTSP ID associated with RTP flows.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtp rtsp-id [case-sensitive] *operator rtsp_id*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

rtsp_id

Specifies the RTSP ID to match.
rtsp_id must be an alphanumeric string of 1 through 32 characters.

Usage

Use this command to define rule expressions to match RTSP ID associated with RTP flows.

Example

The following command defines a rule expression to match RTSP message ID of *test1*:

```
rtp rtsp-id contains test1
```

rtp session-length

This command allows you to define rule expressions to match the total length of RTP sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtp session-length *operator session_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

session_length

Specifies the RTP total session length (in bytes) to match.
In 8.1 and later releases, *session_length* must be an integer from 1 through 4000000000.
In release 8.0, *session_length* must be an integer from 1 through 40000000.

Usage

Use this command to define rule expressions to match the RTP total session length. The session-length is calculated by adding together the “rtp pdu-length” values of all relevant packets.

Example

The following command defines a rule expression to match a total RTP session length of *200000*:

```
rtp session-length = 200000
```

rtp uri

This command allows you to define rule expressions to match the media URI associated with RTP flows.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtp uri [case-sensitive] *operator uri*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

uri

Specifies the RTP URI to match.
uri must be an alphanumeric string of 1 through 127 characters. *uri* allows punctuation characters and excludes the “host” portion.

Usage

Use this command to define rule expressions to match media URI associated with RTP flow.

Example

The following command defines a rule expression to match the RTP URI string *rtsp://www.example.org*:

```
rtp uri = rtsp://www.example.org
```

rtsp any-match

This command allows you to define rule expressions to match all Real Time Streaming Protocol (RTSP) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtsp any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all RTSP packets.

Example

The following command defines a rule expression to match all RTSP packets:

```
rtsp any-match = TRUE
```

rtsp content length

This command allows you to define rule expressions to match the content length field in RTSP header.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtsp content length *operator content_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

content_length

Specifies the content length (in bytes) to match.
content_length must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match “content length” field in RTSP headers.

Example

The following command defines a rule expression to match content length of *10000* in RTSP headers:

```
rtsp content length = 10000
```

rtsp content type

This command allows you to define rule expressions to match the content type field in RTSP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] rtsp content type [ case-sensitive ]` *`operator content_type`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`content_type`

Specifies the content type to match.
`content_type` must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

Usage

Use this command to define rule expressions to match “content type” field in RTSP headers.

Example

The following command defines a rule expression to match RTSP content type *`abc100`*:

```
rtsp content type = abc100
```

rtsp date

This command allows you to define rule expressions to match the date field in the RTSP message headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] rtsp date [ case-sensitive ]` *`operator date`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`date`

Specifies the date in RTSP header to match.
`date` must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the “date” field in the RTSP message headers.

Example

The following command defines a rule expression to match the date *`12_04_2006`* in RTSP message headers:

```
rtsp date = 12_04_2006
```

rtsp previous-state

This command allows you to define rule expressions to match the previous state of RTSP sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtsp previous-state *operator rtsp_previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

rtsp_previous_state

Specifies the previous state to match.
rtsp_previous_state must be one of the following:

- **init**
- **open**
- **play**
- **ready**
- **record**

Usage

Use this command to define rule expressions to match the previous state of RTSP sessions.

Example

The following command defines a rule expression to match RTSP previous state **ready**:

```
rtsp previous-state = ready
```

rtsp reply code

This command allows you to define rule expressions to match the return code in RTSP responses.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtsp reply code *operator reply_code*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

reply_code

Specifies the RTSP reply code to match.
reply_code must be an integer from 100 through 599.

Usage

Use this command to define rule expressions to match the return code in RTSP response.

Example

The following command defines a rule expression to match RTSP return code *302*:

```
rtsp reply code = 302
```

rtsp request method

This command allows you to define rule expressions to match the method in RTSP responses.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtsp request method *operator request_method*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

request_method

Specifies the RTSP request method to match.
request_method must be one of the following requests:

- **announce**
- **describe**
- **get-parameter**
- **options**
- **pause**
- **play**
- **record**
- **redirect**
- **set-parameter**
- **setup**
- **teardown**

Usage

Use this command to define rule expressions to match the method in RTSP responses.

Example

The following command defines a rule expression to match RTSP request method **announce**:

```
rtsp request method = announce
```

rtsp request packet

This command allows you to define rule expressions to match all RTSP request messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtsp request packet *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **TRUE**: Is request
- **FALSE**: Is response

Usage

Use this command to define rule expressions to match all RTSP request messages.

Example

The following command defines a rule expression to match all RTSP request messages:

```
rtsp request packet = TRUE
```

rtsp rtp-seq

This command allows you to define rule expressions to match the “seq” field in the RTP-Info header of RTSP responses.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtsp rtp-seq *operator sequence_number*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

sequence_number

Specifies the sequence number in the RTSP RTP-Info field to match.
sequence_number must be an alphanumeric string of 0 through 65535 characters in Normal Play Time (NPT) time format.

Usage

Use this command to define rule expressions to match user traffic matching the “seq” field in the RTP-Info header of RTSP response for a PLAY request.

Example

The following command defines a rule expression to match user traffic based on RTP-seq number *npt-12:34:59*:

```
rtsp rtp-seq = npt-12:34:59
```

rtsp rtp-time

This command allows you to define rule expressions to match the “time” field in RTP-Info header of RTSP responses.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtsp rtp-time *operator time*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

time

Specifies the time to match.
time must be an alphanumeric string of 1 through 2147483647 characters in Normal Play Time (NPT) time format.

Usage

Use this command to define rule expressions to match the “time” field in the RTP-Info header of RTSP response for a PLAY request.

Example

The following command defines a rule expression to match RTP timestamp of *20120123T153600Z*:

```
rtsp rtp-time = 20120123T153600Z
```

rtsp rtp-uri

This command allows you to define rule expressions to match the URI field in the RTP-Info header of RTSP responses.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] rtsp rtp-uri [ case-sensitive ]` *`operator uri`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`uri`

Specifies the value to match with the URI in RTP-Info header of the RTSP message.
`uri` must be an alphanumeric string of 1 through 127 characters. *`uri`* allows punctuation characters and excludes the “host” portion.

Usage

Use this command to define rule expressions to match the URI field in the RTP-Info header of the RTSP response for a PLAY request.

Example

The following command defines a rule expression to match user traffic based on RTP-URI string *`rtsp://www.foo.com`* in the RTP-info header of RTSP packet:

```
rtsp rtp-uri = rtsp://www.foo.com
```

rtsp session-id

This command allows you to define rule expressions to match the session ID in RTSP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtsp session-id [case-sensitive] *operator session_id*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

session_id

Specifies the session ID to match.
session_id must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match the session ID in RTSP messages.

Example

The following command defines a rule expression to match the RTSP session ID *0123abc100*:

```
rtsp session-id = 0123abc100
```

rtsp session-length

This command allows you to define rule expressions to match the total length of RTSP sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtsp session-length *operator session_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

session_length

Specifies the RTSP session length (in bytes) to match.
session_length must be an integer from 1 through 40000000.

Usage

Use this command to define rule expressions to match the total length of RTSP sessions. That is, the sum of the “rtsp pdu-length” values of all relevant packets.

Example

The following command defines a rule expression to match RTSP session length of *3000000* bytes:

```
rtsp session-length = 3000000
```

rtsp state

This command allows you to define rule expressions to match the current state of RTSP sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtsp state *operator current_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

current_state

Specifies the current state to match.
current_state must be one of the following:

- **end**
- **init**
- **open**
- **play**
- **ready**
- **record**

Usage

Use this command to define rule expressions to match the current state of RTSP sessions.

Example

The following command defines a rule expression to match RTSP current state **init**:

```
rtsp state = init
```

rtsp uri

This command allows you to define rule expressions to match URI in RTSP request message.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtsp uri [case-sensitive] *operator uri*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

uri

Specifies the URI to match.
uri must be an alphanumeric string of 1 through 127 characters. *uri* allows punctuation characters and excludes the “host” portion.

Usage

Use this command to define rule expressions to match URI in RTSP request.

Example

The following command defines a rule expression to match user traffic based on RTSP URI *rtsp://www.example.com:554/twister/audiotrack*:

```
rtsp uri = rtsp://www.example.com:554/twister/audiotrack
```

rtsp uri sub-part

This command allows you to define rule expressions to match user traffic by parsing sub-parts of the URI in an RTSP request message.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] rtsp uri sub-part { { absolute-path | host | query } [case-sensitive] *operator string* **| port {** *port_operator port_value* **| { range | !range }** *range_from* **to** *range_to* **} }**

no

If previously configured, deletes the specified rule expression from the current ruledef.

absolute-path

Specifies the absolute path matching criteria to RTSP URI in an RTSP request message.

host

Specifies the host name matching criteria to RTSP URI in an RTSP request message.

query

Specifies the query string matching criteria to RTSP URI in an RTSP request message.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

string

Specifies the absolute path/host name or query string to match with the URI in RTSP header.

string must be an alphanumeric string of 1 through 127 characters. *string* allows punctuation characters and excludes the “host” portion.

port

Specifies the port related matching for RTSP URI in an RTSP request message.

port_operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

port_value

Specifies the RTSP port number to match with port rule in the RTSP flow as an integer from 0 through 65535.

{ range | !range } *range_from* **to** *range_to* **}**

Enables or disables the range criteria for RTSP flow ports.

- **range**: Enables the range criteria for RTSP flow ports.
- **!range**: Disables the range criteria for RTSP flow ports.
- *range_from*: Specifies the start of range of RTSP flow ports as an integer from 0 through 65535, but less than or equal to *range_to*.
- *range_to*: Specifies the end of range of RTSP flow ports as an integer from 0 through 65535, but more than or equal to *range_from*.

Usage

Use this command to define rule expressions to match URI sub parts like host, absolute path, port, and query in RTSP request messages.

Example

The following command defines a URI sub part rule expression to analyze user traffic based on an RTSP URI port number between *1023* and *1068*:

```
rtsp uri sub-part port range 1023 to 1068
```

rtsp user-agent

This command allows you to define rule expressions to match the user-agent field in RTSP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] rtsp user-agent [ case-sensitive ]` *`operator user_agent`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`user_agent`

Specifies the user agent to match.
`user_agent` must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match the “user-agent” field in RTSP header.

Example

The following command defines a rule expression to match *`test`* in “user-agent” field of RTSP header:

```
rtsp user-agent = test
```

rule-application

This command allows you to specify the purpose of a ruledef, such as for charging, post-processing, routing, and so on.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
rule-application { charging | post-processing | routing | tpo }

no rule-application
```

no

Disables the rule application configuration.

charging

Specifies that the current ruledef is for charging purposes.
Up to 2,048 rule definitions can be defined for the charging application in an Active Charging Service.
Default: Enabled

post-processing

Important: The **post-processing** keyword is available only in 8.3 and later releases.

Specifies that the current ruledef is for post-processing purposes. This enables processing of packets even if the rule matching for them has been disabled.

routing

Specifies that the current ruledef is for routing purposes. Up to 256 rule definitions can be defined for routing in an Active Charging Service. Default: Disabled

tpo

Important: The **tpo** keyword is available only in 12.2 and later releases.

Specifies that the current ruledef is for use in Traffic Performance Optimization (TPO) in-line service's match-rule and match-advertisement configurations.
TPO can use both "charging" and "tpo" ruledefs. Note that ruledef/group-of-ruledef statistics are computed only for TPO ruledefs. For charging ruledefs/group-of-ruledefs, statistics are not computed, and are allowed only for backward compatibility. To enable ruledef statistics, in the TPO policies use "tpo" ruledefs.
Default: Disabled

Usage

Use this command to specify the rule application for a rule definition.
If, when configuring a ruledef, the rule-application is not specified, by default the system configures the ruledef as a charging ruledef.

Example

The following command configures the rule application “charging” to the current rule definition:

```
rule-application charging
```

sdp any-match

This command allows you to define rule expressions to match all packets that contain Session Description Protocol (SDP) descriptions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sdp any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all packets containing SDP descriptions.

Example

The following command defines a rule expression to match all packets containing SDP descriptions:

```
sdp any-match = TRUE
```

sdp connection-ip-address

This command allows you to define rule expressions to match the IP address in the connection field of SDP descriptions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sdp connection-ip-address *operator ip_address*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

ip_address

Specifies the IP address to match.
ip_address must be in IPv4 dotted-decimal notation.

Usage

Use this command to define rule expressions to match IP address in the connection field of SDP descriptions.

Example

The following command defines a rule expression to match the IP address *10.1.1.1* in the connection field of SDP descriptions:

```
sdp connection-ip-address = 10.1.1.1
```

sdp media-audio-port

This command allows you to define rule expressions to match media audio ports specified in the media sections of SDP descriptions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sdp media-audio-port *operator port*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

port

Specifies the port number to match.
port must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match media audio ports specified in the media sections of SDP descriptions.

Example

The following command defines a rule expression to match media audio port *100* in the media sections of SDP descriptions:

```
sdp media-audio-port = 100
```

sdp media-video-port

This command allows you to define rule expressions to match media video ports specified in the media sections of SDP descriptions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sdp media-video-port *operator port*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

port

Specifies the port number to match.
port must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match media video ports specified in the media sections of SDP descriptions.

Example

The following command defines a rule expression to match media video port *100* in the media sections of SDP descriptions:

```
sdp media-video-port = 100
```

sdp uplink

This command allows you to define rule expressions to match SDP descriptions in the uplink (subscriber to network) direction.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sdp uplink *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**: Is not uplink
- **TRUE**: Is uplink

Usage

Use this command to define rule expressions to match SDP descriptions in uplink direction.

Example

The following command defines a rule expression to match all SDP descriptions in the uplink direction:

```
sdp uplink = TRUE
```

secure-http any-match

This command allows you to define rule expressions to match all Secure HTTP (HTTPS) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] secure-http any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all Secure HTTP packets.

Example

The following command defines a rule expression to match all HTTPS packets:

```
secure-http any-match = TRUE
```

secure-http uplink

This command allows you to define rule expressions to match uplink (subscriber to network) HTTPS packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] secure-http uplink *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**: Is not uplink
- **TRUE**: Is uplink

Usage

Use this command to define rule expressions to match uplink HTTPS packets.

Example

The following command defines a rule expression to match all uplink HTTPS packets:

```
secure-http uplink = TRUE
```

sip any-match

This command allows you to define rule expressions to match all Session Initiation Protocol (SIP) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sip any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all SIP packets.

Example

The following command defines a rule expression to match all SIP packets:

```
sip any-match = TRUE
```

sip call-id

This command allows you to define rule expressions to match the Call ID in SIP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sip call-id [case-sensitive] *operator call_id*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

call-id

Specifies the call ID to match.
call-id must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the call ID in SIP messages.

Example

The following command defines a rule expression to match the call ID *test* in SIP messages:

```
sip call-id = test
```

sip content length

This command allows you to define rule expressions to match the content-length field in SIP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sip content length *operator content_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

content_length

Specifies the SIP content length to match.
content_length must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match the content-length field in SIP headers.

Example

The following command defines a rule expression to match the content length *10000* in SIP headers:

```
sip content length = 10000
```

sip content type

This command allows you to define rule expressions to match the content type field in SIP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] sip content type [ case-sensitive ]` *`operator content_type`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`content_type`

Specifies the content type to match.
`content_type` must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match the content type field in SIP headers.

Example

The following command defines a rule expression to match content type *`download_string`* in SIP headers:

```
sip content type = download_string
```

sip from

This command allows you to define rule expressions to match the from field in SIP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sip from [case-sensitive] *operator string*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

string

Specifies the value to match.
string must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the “from” field in SIP messages.

Example

The following command defines a rule expression to match *test1* in the “from” field in SIP messages:

```
sip from contains test1
```

sip previous-state

This command allows you to define rule expressions to match previous state of SIP sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sip previous-state *operator sip_previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

sip_previous_state

Specifies the previous state to match.
sip_previous_state must be one of the following:

- **init**
- **provisional-response**
- **request-sent**
- **response-fail**
- **response-ok**

Usage

Use this command to define rule expressions to match a previous state of SIP sessions.

Example

The following command defines a rule expression to match user traffic based on the SIP previous state of **request-sent**:

```
sip previous-state = request-sent
```

sip reply code

This command allows you to define rule expressions to match the reply code in SIP responses.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sip reply code *operator reply_code*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

reply_code

Specifies the SIP reply code to match.
reply_code must be an integer from 100 through 699.

Usage

Use this command to define rule expressions to match the reply code in SIP responses.

Example

The following command defines a rule expression to match *180* in the reply code in SIP responses:

```
sip reply code = 180
```

sip request method

This command allows you to define rule expressions to match the method in SIP requests.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sip request method *operator method*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

method

Specifies the SIP method to match.
method must be one of the following:

- **ack**
- **bye**
- **cancel**
- **invite**
- **options**
- **register**

Usage

Use this command to define rule expressions to match the method in SIP requests.

Example

The following command defines a rule expression to match the method **bye** in SIP request messages:

```
sip request method = bye
```

sip request packet

This command allows you to define rule expressions to match all SIP request packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sip request packet *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **=**: Equals
- **!=**: Does not equal

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**: Is a response
- **TRUE**: Is a request

Usage

Use this command to define rule expressions to match all SIP request packets.

Example

The following command defines a rule expression to match all SIP request packets:

```
sip request packet = TRUE
```

sip state

This command allows you to define rule expressions to match current state of the SIP session.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sip state *operator current_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

current_state

Specifies the current state to match.
current_state must be one of the following:

- **ack-received**
- **provisional-response**
- **request-sent**
- **response-fail**
- **response-ok**

Usage

Use this command to define rule expressions to match the current SIP session.

Example

The following command defines a rule expression to match user traffic based on SIP current state **request-sent**:

```
sip state = request-sent
```

sip to

This command allows you to define rule expressions to match the “to” field in SIP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] sip to [case-sensitive] *operator to_address*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

to_address

Specifies the “to” address/name to match.
to_address must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the “to” field in SIP messages.

Example

The following command defines a rule expression to match *test1* in the “to” field of SIP messages:

```
sip to contains test1
```

sip uri

This command allows you to define rule expressions to match the URI in SIP messages.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] sip uri [ sub-part { headers | host | parameters | port | userinfo } ] [ case-sensitive ]` *`operator uri`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`sub-part { headers | host | parameters | port | userinfo }`

This is an optional keyword that defines what sub-part of a SIP URI to check.

- **`headers`**: Apply the rule to SIP URI header field.
- **`host`**: Apply the rule the SIP URI host field.
- **`parameters`**: Apply the rule to the SIP URI parameters field.
- **`port`**: Apply the rule to the SIP URI port field.
- **`userinfo`**: Apply the rule to the SIP URI userinfo field.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

The string for sub-part keyword **`port`** must be an integer and requires different operators. Use the following operators with the **`port`** keyword:

- **`!=`**: Does not equal
- **`<=`**: Is less than

- **=**: Equals
- **>=**: Is greater than

uri

Specifies the SIP URI to match.
uri must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters. The string for sub-part keyword **port** must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match the URI in SIP messages.

Example

The following command defines a rule expression to match the URI string *sip:10.1.1.1:5060* in SIP messages:

```
sip uri = sip:10.1.1.1:5060
```

The following command defines a rule expression to match the URI string *sip:nnnn@host:5060;user=phone* in SIP messages:

```
sip uri = sip:nnnn@host:5060;user=phone
```

smtp any-match

This command allows you to define rule expressions to match all Simple Mail Transfer Protocol (SMTP) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] smtp any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all SMTP packets.

Example

The following command defines a rule expression to match all SMTP packets:

```
smtp any-match = TRUE
```

smtp command arguments

This command allows you to define rule expressions to match SMTP command arguments.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] smtp command arguments [ case-sensitive ]` *`operator argument`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`argument`

Specifies the command argument to match.
`argument` must be an alphanumeric string of 1 through 63 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match SMTP command arguments.

Example

The following command defines a rule expression to match SMTP command argument *`test`*:

```
smtp command arguments = test
```

smtp command id

This command allows you to define rule expressions to match SMTP command IDs.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] smtp command id *operator command_id*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

command_id

Specifies the command argument to match.
command_id must be an integer from 0 through 10.

Usage

Use this command to define rule expressions to match SMTP command IDs.

Example

The following command defines a rule expression to match SMTP command ID *8*:

```
smtp command id = 8
```

smtp command name

This command allows you to define rule expressions to match commands sent in SMTP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] smtp command name *operator command_name*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

command_name

Specifies the command name to match.
command_name must be one of the following:

- **bdat**
- **data**
- **ehlo**
- **expn**
- **helo**
- **mail-from**
- **noop**
- **quit**
- **rcpt-to**
- **rset**
- **vrfy**

Usage

Use this command to define rule expressions to match commands sent in SMTP packets.

Example

The following command defines a rule expression to match **data** command in SMTP packets:

```
smtp command name = data
```

smtp mail-size

This command allows you to define rule expressions to match the size of mail sent by a SMTP client.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] smtp mail-size { operator mail_size | { { range | !range } range_from to range_to
} }
```

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

mail_size

Specifies the mail size (in bytes) to match.
mail_size must be an integer from 1 through 40000000.

{ range | !range } *range_from* **to** *range_to*

Enables or disables the range criteria.

- **range**: Enables the range criteria.
- **!range**: Disables the range criteria.
- *range_from*: Specifies the start of range as an integer from 1 through 40000000.
- *range_to*: Specifies the end range. *range_to* must be an integer from 1 through 40000000, and must be greater than *range_from*.

Usage

Use this command to define rule expressions to match the size of mail sent by an SMTP client.

Example

The following command defines a rule expression to match mail size of *40000* bytes:

```
smtp mail-size = 40000
```

smtp pdu-length

This command allows you to define rule expressions to match the Protocol Data Unit (PDU) length of SMTP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] smtp pdu-length { *operator pdu_length* **| { { range | !range }** *range_from* **to** *range_to* **} }**

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

---

pdu_length

Specifies the SMTP PDU length (in bytes) to match.
pdu_length must be an integer from 1 through 65535.

{ range | !range } *range_from* **to** *range_to*

Enables or disables the range criteria.

- **range**: Enables the range criteria.
- **!range**: Disables the range criteria.
- *range_from*: Specifies the start of range as an integer from 1 through 65535.
- *range_to*: Specifies the end range. *range_to* must be an integer from 1 through 65535, and must be greater than *range_from*.

Usage

Use this command to define rule expressions to match PDU length of SMTP packets, that is headers + payload.

Example

The following command defines a rule expression to match a PDU length of *1600* bytes:

```
smtp pdu-length = 1600
```

smtp previous-state

This command allows you to define rule expressions to match previous state of SMTP command sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] smtp previous-state *operator smtp_previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

smtp_previous_state

Specifies the previous state to match.
smtp_previous_state must be one of the following:

- **close**: Closed state
- **init**: Initialized state
- **response-error**: Reply error state
- **response-ok**: Response ok state
- **waiting-for-response**: Waiting for response state

Usage

Use this command to define rule expressions to match a previous state of SMTP command sessions.

Example

The following command defines a rule expression to match user traffic based on SMTP previous state **close**:

```
smtp previous-state = close
```

smtp recipient

This command allows you to define rule expressions to match the recipient e-mail ID in the current SMTP transaction.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] smtp recipient [ case-sensitive ]` *`operator argument`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`case-sensitive`

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`argument`

Specifies the response argument to match.
`argument` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the recipient e-mail ID in the current SMTP transaction.

Example

The following command defines a rule expression to match recipient e-mail ID containing *`test`* in the current SMTP transaction:

```
smtp recipient contains test
```

smtp reply arguments

This command allows you to define rule expressions to match the arguments within SMTP responses.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] smtp reply arguments [case-sensitive] *operator argument*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

argument

Specifies the reply argument to match.
argument must be an alphanumeric string of 1 through 63 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the arguments with SMTP response.

Example

The following command defines a rule expression to match reply argument *forward-path* in SMTP response:

```
smtp reply arguments = forward-path
```

smtp reply id

This command allows you to define rule expressions to match reply ID assigned to SMTP responses.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] smtp reply id` *`operator reply_id`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`=`**: Equals

`reply_id`

Specifies the reply ID to match.
`reply_id` must be one of the following:

- **`0`**: +NO reply
- **`1`**: +OK reply
- **`2`**: -ERR reply

Usage

Use this command to define rule expressions to reply ID assigned to SMTP response.

Example

The following command defines a rule expression to match reply ID *`2`* assigned to SMTP response:

```
smtp reply id = 2
```

smtp reply status

This command allows you to define rule expressions to match the reply status in SMTP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] smtp reply status *operator reply_status*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

reply_status

Specifies the SMTP reply status to match.
reply_status must be one of the following:

- **+OK**: Response OK
- **-ERR**: Response error

Usage

Use this command to define rule expressions to match reply status in SMTP packets.

Example

The following command defines a rule expression to match reply status **+OK** in SMTP packets:

```
smtp reply status = +OK
```

smtp sender

This command allows you to define rule expressions to match sender e-mail ID in the current SMTP transaction.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] smtp sender [case-sensitive] *operator sender*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

sender

Specifies the sender value to match.
sender must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match sender e-mail ID in the current SMTP transaction.

Example

The following command defines a rule expression to match sender e-mail ID containing *test* in the current SMTP transaction:

```
smtp sender contains test
```

smtp session-length

This command allows you to define rule expressions to match total length of SMTP sessions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] smtp session-length { *operator session_length* **| { range | !range }** *range_from* **to** *range_to* **}**

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

session_length

Specifies the session length to match.
session_length must be an integer from 1 through 40000000.

{ range | !range } *range_from* **to** *range_to*

Enables or disables the range criteria.

- **range**: Enables the range criteria.
- **!range**: Disables the range criteria.
- *range_from*: Specifies the start of range as an integer from 1 through 40000000.
- *range_to*: Specifies the end range. *range_to* must be an integer from 1 through 40000000, and must be greater than *range_from*.

Usage

Use this command to define rule expressions to match total length of SMTP session.

Example

The following command defines a rule expression to match SMTP session length of *4000000*:

```
smtp session-length = 4000000
```

smtp state

This command allows you to define rule expressions to match current state of a SMTP command session.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] smtp state *operator current_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

current_state

Specifies the current state to match.
current_state must be one of the following:

- **close**: Closed state
- **init**: Initialized state
- **response-error**: Response of error state
- **response-ok**: Response of ok state
- **waiting-for-response**: Waiting for response state

Usage

Use this command to define rule expressions to match current state of SMTP command session.

Example

The following command defines a rule expression to match current state as **close** of SMTP command session:

```
smtp state = close
```

tcp analyzed out-of-order

This command allows you to define rule expressions to determine whether the received TCP packet was received before all of the earlier sequenced packets have been received. This functionality is for whether the packet was analyzed or discarded because the earlier sequenced packet(s) was (were) not received before a timeout expired.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

`[ no ] tcp analyzed out-of-order` *`operator condition`*

`no`

If previously configured, deletes the specified rule expression from the current ruledef.

`operator`

Specifies how to match.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`=`**: Equals

`condition`

Specifies the condition to match.
`condition` must be one of the following:

- **`FALSE`**: Not analyzed
- **`TRUE`**: Analyzed

Usage

This command is used to set the status flag to ‘analyzed’ or ‘not analyzed’ for all TCP packets received at the ACSMgr/SessMgr prior to their earlier packets.
When a packet reaches ACSMgr/SessMgr prior to earlier packet(s), it and subsequent packets are buffered at ACSMgr/SessMgr as TCP out-of-order packets and ACSMgr/SessMgr waits for missing packet(s) until the time-out duration expires. If the packet(s) with the missing sequence number(s) arrives within the time-out duration, all buffered packets with the correct sequence will be presented to upper layers (HTTP etc.) for analysis; otherwise buffered TCP out-of-order packets will be sent to charging with analysis done flag at the TCP/IP layer only.
If this command is enabled the TCP out-of-order packets are marked and sent to TCP analyzer as analyzed for charging action, otherwise they are discarded.

Example

The following command sets to analyze TCP out-of-order packets:

```
tcp analyzed out-of-order = TRUE
```

tcp any-match

This command allows you to define rule expressions to match all TCP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**: Not analyzed
- **TRUE**: Analyzed

Usage

Use this command to define rule expressions to match all TCP packets.

Example

The following command defines a rule expression to match all TCP packets:

```
tcp any-match = TRUE
```

tcp connection-initiator

This command allows you to define rule expressions to match the TCP connection initiator.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] tcp connection-initiator operator subscriber
```

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

subscriber

Specifies that the connection is being initiated by the subscriber.

Usage

Use this command to define rule expressions to match the TCP connection initiator, and to allow the operator to differentiate when the connection initiated by subscriber or the subscriber is acting as a Transaction Control Server (TCS) server.

Example

The following command defines a rule expression to match user traffic based on TCP connection initiator **subscriber**:

```
tcp connection-initiator = subscriber
```

tcp downlink

This command allows you to define rule expressions to match downlink (network to subscriber) TCP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp downlink *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match downlink (to subscriber) TCP packets.

Example

The following command defines a rule expression to match downlink TCP packets:

```
tcp downlink = TRUE
```

tcp dst-port

This command allows you to define rule expressions to match destination port number in TCP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp dst-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map_name* **} }**

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

---

port_number

Specifies the port number to match.
port_number must be an integer from 1 through 65535.

---

range | !range

Specifies the range criteria:

- **!range**: Not in the range
- **range**: In the range

---

start_range **to** *end_range*

Specifies the starting and ending port numbers for the range of destination TCP ports.

- *start_range* must be an integer from 1 through 65535.
- *end_range* must be an integer from 1 through 65535, and must be greater than *start_range*.

---

port-map *port_map_name*

Specifies the port map for the port range. *port_map_name* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define rule expressions to match destination port number in TCP headers.

Example

The following command defines a rule expression to match destination port number *10* in TCP headers:

```
tcp dst-port = 10
```

tcp duplicate

This command allows you to define rule expressions to match TCP retransmissions.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] tcp duplicate operator condition
```

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**: Not duplicated/retransmitted
- **TRUE**: Duplicated/retransmitted

Usage

Use this command to specify rule expressions to match TCP retransmission.

Example

The following command defines a rule expression to match TCP retransmissions:

```
tcp duplicate = TRUE
```

tcp either-port

This command allows you to define rule expressions to match either a destination or source port number in TCP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp either-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map_name* **} }**

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

---

port_number

Specifies the port number to match.
port_number must be an integer from 1 through 65535.

---

range | !range

Specifies the range criteria:

- **!range**: Not in the range
- **range**: In the range

---

start_range **to** *end_range*

Specifies the starting and ending port numbers for the port range.

- *start_range* must be an integer from 1 through 65535.
- *end_range* must be an integer from 1 through 65535, and must be greater than *start_range*.

---

port-map *port_map_name*

Specifies the port map for the port range. *port_map_name* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define rule expressions to match either a destination or source port number in TCP headers.
This command expression allows you to create a single ruledef using either-port, rather than needing two ruledefs (one with dst-port and one with src-port).

Example

The following command defines a rule expression to match destination/source port number *10* in TCP header:

```
tcp either-port = 10
```

tcp error

This command allows you to define rule expressions to identify errors, either in the packet (for example, TCP checksum error) or in the TCP analyzer's Finite State Machine (FSM).

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp error *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define a rule expression to identify errors, either in the packet (for example, TCP checksum error) or in the TCP analyzer's FSM.

Example

The following command defines a rule expression to match TCP errors:

```
tcp error = TRUE
```

tcp flag

This command allows you to define rule expressions to match bit within the flag field of TCP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] tcp flag operator flag
```

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!contains**: Does not contain
- **contains**: Contains
- **!=**: Does not equal
- **=**: Equals

flag

Specifies the flag value to match.
flag must be one of the following:

- **ack**: TCP FLAG ACK
- **fin**: TCP FLAG FIN
- **push**: TCP FLAG PUSH
- **reset**: TCP FLAG RESET
- **syn**: TCP FLAG SYN

Usage

Use this command to define rule expressions to match a bit within the flag field of TCP headers.

Example

The following command defines a rule expression to match **reset** within flag field of TCP headers:

```
tcp flag = reset
```

tcp initial-handshake-lost

This command allows you to define rule expressions to match data packets when there has been no TCP handshaking to establish TCP connection.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp initial-handshake-lost *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match data packets when there has been no TCP handshaking to establish TCP connection.

Example

The following command defines a rule expression to identify TCP flow where the initial handshake was not seen:

```
tcp initial-handshake-lost = TRUE
```

tcp payload

This command allows you to define rule expressions to match hexadecimal or ASCII string content in the payload protocol-signature field of the TCP payload.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp payload starts-with { hex-signature *hex_string* **| string-signature** *string* **}**

no

If previously configured, deletes the specified rule expression from the current ruledef.

hex-signature *hex_string*

Specifies hexadecimal protocol signature in payload field.
hex_string must be a dash-delimited list of hex data of size smaller than 32.

string-signature *string*

Specifies protocol signature in payload field.
string must be an alphanumeric string of 1 through 32 characters.

Usage

Use this command to define rule expressions to match for Hex/ASCII string content in payload protocol-signature field.
This rule expression is useful for detecting certain applications.

Example

The following command defines a rule expression to identify user traffic based on TCP protocol signature *tcp1*:

```
tcp payload starts-with string-signature tcp1
```

tcp payload-length

This command allows you to define rule expressions to match the length of a TCP payload.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp payload-length *operator payload_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

payload_length

Specifies the TCP payload length to match.
payload_length must be an integer from 0 through 40000000.

Usage

Use this command to define rule expressions to match length of TCP payload, excluding the TCP or lower layer headers.
To match TCP control packets configure a payload-length of 0 (zero).

Example

The following command defines a rule expression to match TCP payload length of *10000*:

```
tcp payload-length = 10000
```

tcp previous-state

This command allows you to define rule expressions to match previous state of TCP connections.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp previous-state *operator tcp_previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

tcp_previous_state

Specifies the previous state to match.
tcp_previous_state must be one of the following:

- **close**
- **close-wait**
- **closing**
- **established**
- **fin-wait1**
- **fin-wait2**
- **last-ack**
- **listen**
- **syn-received**
- **syn-sent**
- **time-wait**

Usage

Use this command to define rule expressions to match a TCP previous state.

Example

The following command defines a rule expression to match user traffic based on previous state **time-wait**:

```
tcp previous-state = time-wait
```

tcp proxy-prev-state

This command allows you to define rule expressions to match TCP previous state on the ingress side of the TCP proxy.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp proxy-prev-state *operator previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

previous_state

Specifies the previous state to match.
previous_state must be one of the following:

- **close**
- **close-wait**
- **closing**
- **established**
- **fin-wait1**
- **fin-wait2**
- **last-ack**
- **listen**
- **syn-received**
- **syn-sent**
- **time-wait**

Usage

If there is no TCP proxy configured, this configuration is not applicable.
For proxy-enabled flows, TCP state handling interprets the ingress side as the radio side and the egress side as the Internet side of the TCP connection.
tcp state and **tcp prev-state** is the state of the client stack, which would be either the state of the subscriber's stack (if flow is not proxy enabled) or the MS state of proxy on the egress-side (if flow is proxy-enabled).

tcp proxy-state and **tcp proxy-prev-state** is the state of the embedded TCP proxy server, that is the proxy ingress-side.
So, depending on the use case, if using **tcp state** and **tcp prev-state** an existing configuration may work fine regardless of whether proxy is enabled. For other use cases, other ruledefs may have to be created. Both **tcp state** and **tcp proxy-state** can be used in the same ruledef. If proxy was being used, they would map to the egress-side and ingress-side, respectively. If proxy was not being used, then this would not match ruledef because proxy state would not be applicable.

Example

The following command defines a rule expression to match user traffic based on TCP proxy previous state of established:

```
tcp proxy-prev-state = established
```

tcp proxy-state

This command allows you to define rule expressions to match the TCP state on the ingress side of the TCP proxy.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp proxy-state *operator state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

state

Specifies the state to match.
state must be one of the following:

- **close**
- **close-wait**
- **closing**
- **established**
- **fin-wait1**
- **fin-wait2**
- **last-ack**
- **listen**
- **syn-received**
- **syn-sent**
- **time-wait**

Usage

If there is no TCP proxy configured, this configuration is not applicable.
For proxy-enabled flows, TCP state handling interprets the ingress side as the radio side and the egress side as the Internet side of the TCP connection.
tcp state and **tcp prev-state** is the state of the client stack, which would be either the state of the subscriber's stack (if flow is not proxy enabled) or the MS state of proxy on egress-side (if flow is proxy-enabled).

tcp proxy-state and **tcp proxy-prev-state** is the state of the embedded TCP proxy server, that is the proxy ingress-side.
So, depending on the use case, if using **tcp state** and **tcp prev-state** an existing configuration may work fine regardless of whether proxy is enabled. For other use cases, other ruledefs may have to be created. Both **tcp state** and **tcp proxy-state** can be used in the same ruledef. If proxy was being used, they would map to the egress-side and ingress-side, respectively. If proxy was not being used, then this would not match the ruledef because proxy state would not be applicable.

Example

The following command defines a rule expression to match user traffic based on TCP proxy previous state of established:

```
tcp proxy-state = established
```

tcp session-length

This command allows you to define rule expressions to match the total length of a TCP session.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp session-length *operator session_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

session_length

Specifies the TCP session length (in bytes) to match as be an integer from 0 through 4000000000.

Usage

Use this command to define rule expressions to match the total length of a TCP session.
The session-length is calculated by adding together the TCP payload-length values of all relevant packets.

Example

The following command defines a rule expression to match user traffic based on TCP session length of *2000* bytes:

```
tcp session-length = 2000
```

tcp src-port

This command allows you to define rule expressions to match source a port number in TCP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp src-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map_name* **} }**

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

---

port_number

Specifies the port number to match.
port_number must be an integer from 1 through 65535.

---

range | !range

Specifies the range criteria:

- **!range**: Not in the range
- **range**: In the range

---

start_range **to** *end_range*

Specifies the starting and ending port numbers for the port range.

- *start_range* must be an integer from 1 through 65535.
- *end_range* must be an integer from 1 through 65535, and must be greater than *start_range*.

---

port-map *port_map_name*

Specifies the port map for the port range. *port_map_name* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define rule expressions to match source a port number in TCP headers.

Example

The following command defines a rule expression to analyze user traffic matching TCP source port *10*:

```
tcp src-port = 10
```

tcp state

This command allows you to define rule expressions to match current state of TCP connections.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp state *operator current_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

current_state

Specifies the current state to match.
current_state must be one of the following:

- **close**
- **close-wait**
- **closing**
- **established**
- **fin-wait1**
- **fin-wait2**
- **last-ack**
- **listen**
- **syn-received**
- **syn-sent**
- **time-wait**

Usage

Use this command to define rule expressions to match a current state of TCP connections.

Example

The following command defines a rule expression to match user traffic based on current state **close**:

```
tcp state = close
```

tcp uplink

This command allows you to define rule expressions to match uplink (subscriber to network) TCP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tcp uplink *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to uplink TCP packets.

Example

The following command defines a rule expression to uplink TCP packets:

```
tcp uplink = TRUE
```

tethering-detection

This command allows you to define rule expressions to match tethered or non-tethered flows.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

tethering-detection { flow-not-tethered | flow-tethered }

no tethering-detection

no

Deletes the tethering detection configuration from the ruledef.

flow-not-tethered

Specifies to match if tethering is not detected on flow.

flow-tethered

Specifies to match if tethering is detected on flow.

Usage

Use this command to define rule expressions to match tethered/non-tethered flows.
Note that in order for the rule containing the tethering-detection configuration to get matched, at least one valid rule line has to be present in it.
This configuration is treated in a special manner by the rule matching engine in that it is excluded from the condition **multi-line-or all-lines**. For example, if there are three rule-lines in a ruledef and multi-line-or is enabled as follows:

```
ruledef all-tethered-web-traffic

   http any-match = TRUE

   wsp any-match = TRUE

   multi-line-or all-lines

   tethering-detection flow-tethered

   exit
```

In this case, if for a packet only the rule line **tethering-detection flow-tethered** matches, it is not sufficient to result in a rule match even though **multi-line-or all-lines** is enabled in the ruledef.

Example

The following command defines a rule expression to match tethered flows:

tethering-detection flow-tethered

tftp any-match

This command allows you to define rule expressions to match all Trivial File Transfer Protocol (TFTP) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] tftp any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**: Not analyzed
- **TRUE**: Analyzed

Usage

Use this command to define rule expressions to match all TFTP packets.

Example

The following command defines a rule expression to match all TFTP packets:

```
tftp any-match = TRUE
```

tftp data-any-match

This command allows you to define rule expressions to match all TFTP data packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] tftp data-any-match operator condition
```

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**: Not analyzed
- **TRUE**: Analyzed

Usage

Use this command to define rule expressions to match all TFTP data packets.

Example

The following command defines a rule expression to match all TFTP data packets:

```
tftp data-any-match = TRUE
```

udp any-match

This command allows you to define rule expressions to match all UDP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] udp any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all UDP packets.

Example

The following command defines a rule expression to match all UDP packets:

```
udp any-match = TRUE
```

udp downlink

This command allows you to define rule expressions to match downlink (network to subscriber) UDP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] udp downlink operator condition
```

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match downlink UDP packets.

Example

The following command defines a rule expression to match downlink UDP packets:

```
udp downlink = TRUE
```

udp dst-port

This command allows you to define rule expressions to match destination port number in UDP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] udp dst-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map_name* **} }**

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

---

port_number

Specifies the port number to match.
port_number must be an integer from 1 through 65535.

!range | range

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

---

start_range **to** *end_range*

Specifies the starting and ending port numbers for the port range.

- *start_range* must be an integer from 1 through 65535.
- *end_range* must be an integer from 1 through 65535, and must be greater than *start_range*.

---

port-map *port_map_name*

Specifies the port map for the port range. *port_map_name* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define rule expressions to match destination port number in UDP headers.

Example

The following command defines a rule expression to match user traffic based on destination port number *10*:

```
udp dst-port = 10
```

udp either-port

This command allows you to define rule expressions to match either a destination or source port number in UDP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] udp either-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map_name* **} }**

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

---

port_number

Specifies the port number to match.
port_number must be an integer from 1 through 65535.

!range | range

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

---

start_range **to** *end_range*

Specifies the starting and ending port numbers for the port range.
start_range must be an integer from 1 through 65535.
end_range must be an integer from 1 through 65535, and must be greater than *start_range*.

---

port-map *port_map_name*

Specifies the port map for the port range. *port_map_name* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define rule expressions to match either destination or source port number in UDP headers.

Example

The following command defines a rule expression to match user traffic based on match either source/destination port number *10*:

```
udp either-port = 10
```

udp payload starts-with

This command allows you to define rule expressions to match hex/ASCII string content in UDP payload protocol-signature field.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] udp payload starts-with { hex-signature *hex_string* **| string-signature** *string* **}**

no

If previously configured, deletes the specified rule expression from the current ruledef.

hex-signature *hex_string*

Specifies hexadecimal protocol signature in payload field.
hex_string must be a dash-delimited list of hex data of size smaller than 32.

string-signature *string*

Specifies protocol signature in payload field.
string must be an alphanumeric string of 1 through 32 characters.

Usage

Use this command to define rule expressions to match for Hex/ASCII string content in UDP payload protocol-signature field.
This rule expression is useful for detecting certain applications.

Example

The following command defines a UDP rule expression to analyze user traffic based on UDP protocol signature *udp1*:

```
udp payload starts-with string-signature udp1
```

udp src-port

This command allows you to define rule expressions to match source port number in UDP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] udp src-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map_name* **} }**

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

---

port_number

Specifies the port number to match.
port_number must be an integer from 1 through 65535.

!range | range

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

---

start_range **to** *end_range*

Specifies the starting and ending port numbers for the port range.
start_range must be an integer from 1 through 65535.
end_range must be an integer from 1 through 65535, and must be greater than *start_range*.

---

port-map *port_map_name*

Specifies the port map for the port range. *port_map_name* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define rule expressions to match source port number in UDP headers.

Example

The following command defines a rule expression to match source port number *10* in UDP headers:

```
udp src-port = 10
```

udp uplink

This command allows you to define rule expressions to match uplink (subscriber to network) UDP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] udp uplink *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match uplink UDP packets.

Example

The following command defines a rule expression to match uplink (from subscriber) UDP packets:

```
udp uplink = TRUE
```

wsp any-match

This command allows you to define rule expressions to match all Wireless Session Protocol (WSP) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to specify a rule expression to match all WSP packets.

Example

The following command defines a rule expression to match all WSP packets:

```
wsp any-match = TRUE
```

wsp content type

This command allows you to define rule expressions to match the content type field in WSP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp content type [case-sensitive] *operator content_type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

content_type

Specifies content type to match.
content_type must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match “content type” field in WSP headers.

Example

The following command defines a rule expression to WSP content type *test*:

```
wsp content type = test
```

wsp domain

This command allows you to define rule expressions to match domain portion of the URI for WSP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp domain [case-sensitive] *operator domain*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

domain

Specifies the domain to match.
domain must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match the domain portion of URIs in WSP packets. From the URL, after http:// (if present) is removed, everything until the first "/" is the domain.

Example

The following command defines a rule expression to match user traffic based on domain name *testdomain*:

```
wsp domain = testdomain
```

wsp downlink

This command allows you to define rule expressions to match downlink (network to subscriber) WSP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp downlink *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the downlink (from the Mobile Node direction) status to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match downlink WSP packets.

Example

The following command defines a rule expression to match downlink WSP packets:

```
wsp downlink = TRUE
```

wsp first-request-packet

This command allows you to define rule expressions to match WSP first-request-packet.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp first-request-packet *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match the GET or POST request, if it is the first WSP request for the subscriber's session.

Example

The following command defines a rule expression to match WSP first-request-packet:

```
wsp first-request-packet = TRUE
```

wsp host

This command allows you to define rule expressions to match the host name header field in WSP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp host [case-sensitive] *operator host_name*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

host_name

Specifies the WSP host name to match.
host_name must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match host name header field in WSP headers.

Example

The following command defines a rule expression to match host name *host1* in WSP headers:

```
wsp host contains host1
```

wsp pdu-length

This command allows you to define rule expressions to match WSP PDU length.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp pdu-length *operator pdu_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

pdu_length

Specifies the WSP PDU length (in bytes) to match.
pdu_length must be an integer from 1 through 65535.

Usage

Use this command to define rule expressions to match WSP PDU length (header + payload) in bytes.

Example

The following command defines a rule expression to match user traffic based on WSP PDU length of *10000* bytes:

```
wsp pdu-length = 10000
```

wsp pdu-type

This command allows you to define rule expressions to match WSP PDU type in the current packet.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp pdu-type *operator pdu_type*

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

---

pdu_type

Specifies the WSP PDU type to match.
pdu_type must be one of the following:

- **confirmed push**
- **connect-reply**
- **connect-request**
- **data-fragment**
- **delete**
- **disconnect**
- **get**
- **head**
- **options**
- **post**
- **push**
- **put**
- **redirect**
- **reply**
- **resume**
- **suspend**
- **trace**

Usage

Use this command to define rule expressions to match WSP PDU type value in current packet.

Example

The following command defines a rule expression to match WSP PDU type **resume**:

```
wsp pdu-type resume
```

wsp previous-state

This command allows you to define rule expressions to match previous WSP method invocation state.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp previous-state *operator wsp_previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

wsp_previous_state

Specifies the previous state to match.
wsp_previous_state must be one of the following:

- **init**
- **response-error**
- **response-ok**
- **waiting-for-response**

Usage

Use this command to define rule expressions to match WSP previous state.

Example

The following command defines a rule expression to match WSP previous state of *response-ok*:

```
wsp previous-state = response-ok
```

wsp reply code

This command allows you to define rule expressions to match WSP reply code.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp reply code *operator reply_code*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

reply_code

Specifies the WSP reply code to match.
reply_code must be an integer from 0 through 101.

Usage

Use this command to define rule expressions to match WSP reply code.

Example

The following command defines a rule expression to match WSP reply code of *50*:

```
wsp reply code = 50
```

wsp session-length

This command allows you to define rule expressions to match total length of a WSP session.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp session-length *operator session_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: less than equals
- **=**: Equals
- **>=**: greater than equals

session_length

Specifies the WSP session length (in bytes) to match.
session_length must be an integer from 1 through 65535.

Usage

Use this command to define rule expressions to match total length of WSP session.

Example

The following command defines a rule expression to match WSP session length of *2000* bytes:

```
wsp session-length = 2000
```

wsp session-management

This command allows you to define rule expressions to match WSP Session Management state.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp session-management { previous-state | state } *operator state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

previous-state

Specifies the previous WSP Session Management state.

state

Specifies current WSP Session Management Finite State Machine (FSM) state.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

state

Specifies the state to match.
For **previous-state**, *state* must be one of the following:

- **connected**
- **connecting**
- **init**
- **resuming**
- **suspended**

For **state**, *state* must be one of the following:

- **close**
- **connected**
- **connecting**
- **init**
- **resuming**
- **suspended**

Usage

Use this command to define rule expressions to match a WSP Session Management state.

Example

The following command defines a rule expression to match previous WSP Session Management state of **connecting**:

```
wsp session-management previous-state = connecting
```

wsp state

This command allows you to define rule expressions to match WSP Method Invocation state.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp state *operator current_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

current_state

Specifies the current state to match.
current_state must be one of the following:

- **close**
- **response-error**
- **response-ok**
- **waiting-for-response**

Usage

Use this command to define rule expressions to match WSP Method Invocation state.

Example

The following command defines a rule expression to match a WSP Method Invocation state **close**:

```
wsp state = close
```

wsp status

This command has been deprecated. See the **wsp reply-code**command.

wsp tid

This command allows you to define rule expressions to match Transaction Identifier (TID) field for connection-less WSP.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp tid *operator transaction_id*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

transaction_id

Specifies the transaction identifier to match.
transaction_id must be an integer from 0 through 255.

Usage

Use this command to define rule expressions to match TID field for connection-less WSP.

Example

The following command defines a rule expression to match a TID value of *22* for connection-less WSP:

```
wsp tid = 22
```

wsp total-length

This command has been deprecated. See the **wsp session-length** command.

wsp transfer-encoding

This command allows you to define rule expressions to match transfer encoding present in WSP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp transfer-encoding [case-sensitive] *operator transfer_encoding*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

transfer_encoding

This must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match transfer encoding present in WSP header.

Example

The following command defines a rule expression to match user traffic based on WSP transfer encoding 7:

```
wsp transfer-encoding contains 7
```

wsp uplink

This command allows you to define rule expressions to match uplink (subscriber to network) WSP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp uplink *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the uplink (to the Mobile Node direction) status to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match uplink WSP packets.

Example

The following command defines a rule expression to match uplink WSP packets:

```
wsp uplink = TRUE
```

wsp url

This command allows you to define rule expressions to match WSP URL.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp url [case-sensitive] *operator url*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

url

Specifies the URL to match.
url must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match the complete URL, including the host portion.

Example

The following command defines a rule expression to match user traffic based on WSP URL *wsp://wiki.tcl.tk*:

```
wsp url = wsp://wiki.tcl.tk
```

wsp user-agent

This command allows you to define rule expressions to match user agent field in WSP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp user-agent [case-sensitive] *operator user_agent*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

user_agent

Specifies the WSP user agent to match.
user_agent must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match a user agent field in WSP headers.

Example

The following command defines a rule expression to match value *test* in user agent field in WSP headers:

```
wsp user-agent contains test
```

wsp x-header

This command allows you to define rule expressions to match WSP extension-headers (x-headers).

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wsp x-header *name* **[case-sensitive]** *operator string*

no

If previously configured, deletes the specified rule expression from the current ruledef.

name

Specifies the x-header value as an alphanumeric string of 1 through 31 characters.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

string

Specifies the value of the extension header as an alphanumeric string of 1 through 127 characters.

Usage

Use this command to configure any x-header field in WSP and parse it. The extension-header mechanism allows additional header fields to be defined without changing the protocol. The extension-header can be any header fields that are not specified in the RFC standard.

Example

The following command defines a rule expression to analyze user traffic containing WSP extension-header of *test_field* and value of *test_string*:

```
wsp x-header test_field = test_string
```

wtp any-match

This command allows you to define rule expressions to match all Wireless Transaction Protocol (WTP) packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wtp any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all WTP packets.

Example

The following command defines a rule expression to match all WTP packets:

```
wtp any-match = TRUE
```

wtp downlink

This command allows you to define rule expressions to match downlink (network to subscriber) WTP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wtp downlink *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the downlink (from the Mobile Node direction) status to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match downlink WTP packets.

Example

The following command defines a rule expression to match all downlink WTP packets:

```
wtp downlink = TRUE
```

wtp gtr

This command allows you to define rule expressions to match Group Transmission (GTR) flag in the current WTP PDU.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wtp gtr *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match the GTR flag (that indicates the last packet of a packet group) in the current WTP PDU.

Example

The following command defines a rule expression to match WTP user traffic based on WTP GTR:

```
wtp gtr = TRUE
```

wtp pdu-length

This command allows you to define rule expressions to match WTP PDU length.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wtp pdu-length *operator pdu_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

pdu_length

Specifies the WTP PDU length (in bytes) to match.
pdu_length must be an integer from 1 through 65535.

Usage

Use this command to define rule expressions to match WTP PDU length (header + payload) in bytes.

Example

The following command defines a rule expression to match WTP PDU length of *9647* bytes:

```
wtp pdu-length = 9647
```

wtp pdu-type

This command allows you to define rule expressions to match WTP PDU type.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wtp pdu-type *operator pdu_type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

pdu_type

Specifies the WTP PDU type to match.
pdu_type must be one of the following:

- **abort**
- **ack**
- **invoke**
- **negative-ack**
- **result**
- **segment-invoke**
- **segment-result**

Usage

Use this command to define rule expressions to match WTP PDU type.

Example

The following command defines a rule expression to match the WTP PDU type **result**:

```
wtp pdu-type = result
```

wtp previous-state

This command allows you to define rule expressions to match previous WTP state.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wtp previous-state *operator wtp_previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

wtp_previous_state

Specifies the previous state to match.
wtp_previous_state must be one of the following:

- **ack-sent**
- **init**
- **invoke-sent**
- **rcvd**
- **result-rcvd**

Usage

Use this command to define rule expressions to match WTP previous state.

Example

The following command defines a rule expression to match user traffic based on WTP previous state of **ack-sent**:

```
wtp previous-state = ack-sent
```

wtp rid

This command allows you to define rule expressions to match Re-transmission Indicator (RID) flag set in WTP traffic.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wtp rid *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match WTP RID flag.

Example

The following command defines a rule expression to match user traffic containing WTP RID flag:

```
wtp rid = TRUE
```

wtp state

This command allows you to define rule expressions to match current WTP state.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wtp state *operator current_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

current_state

Specifies the current state to match.
current_state must be one of the following:

- **ack-sent**
- **close**
- **init**
- **invoke-sent**
- **rcvd**
- **result-rcvd**

Usage

Use this command to define rule expressions to match current WTP state.

Example

The following command defines a rule expression to match user traffic based on current WTP state **close**:

```
wtp state = close
```

wtp tid

This command allows you to define rule expressions to match WTP Transaction Identifier (TID).

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wtp tid *operator transaction_id*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

transaction_id

Specifies the transaction identifier to match.
transaction_id must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match WTP TID. This expression ignores the high order bit in the protocol that indicates the direction.

Example

The following command defines a rule expression to match user traffic containing WTP TID value of *22*:

```
wtp tid = 22
```

wtp transaction class

This command allows you to define rule expressions to match WTP Transaction Class (TCL) state.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wtp transaction class *operator transaction_class*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

transaction_class

Specifies the WTP TCL to match.
transaction_class must be an integer from 0 through 2.

Usage

Use this command to define rule expressions to match WTP transaction class.

Example

The following command defines a rule expression to match WTP traffic based on WTP transaction class *2*:

```
wtp transaction class = 2
```

wtp ttr

This command allows you to define rule expressions to match WTP Trailer Transmission (TTR) flag.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wtp ttr *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match TTR flag (used to indicate the last packet in a segmented message) in the current WTP PDU.

Example

The following command defines a rule expression to match WTP traffic based on the presence of the WTP TTR flag:

```
wtp ttr = TRUE
```

wtp uplink

This command allows you to define rule expressions to match uplink (subscriber to network) WTP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] wtp uplink *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match uplink WTP packets.

Example

The following command defines a rule expression to match all uplink WTP packets:

```
wtp uplink = TRUE
```

www any-match

This command allows you to define rule expressions to match all WWW packets. It is true for HTTP, WAP1.x, and WAP2.0 protocols.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] www any-match *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match all WWW packets. This expression is true for HTTP, WAP1.x, and WAP2.0 protocols

Example

The following command defines a rule expression to match all WWW packets:

```
www any-match = TRUE
```

www content type

This command allows you to define rule expressions to match the Content-Type field of HTTP/WSP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] www content type [case-sensitive] *operator content_type*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

content_type

Specifies the value to match.
content_type must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the “content type” field of HTTP/WSP header.

Example

The following command defines a rule expression to match the WWW content type *Accept*:

```
www content type = Accept
```

www domain

This command allows you to define rule expressions to match the domain portion of URIs in WSP/HTTP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] www domain [case-sensitive] *operator domain*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

domain

Specifies the domain to match.
domain must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match the domain portion of URIs in WSP/HTTP packets. From the URL, after http:// (if present) is removed, everything until the first "/" is the domain.

Example

The following command defines a rule expression to match user traffic based on domain name *testdomain*:

```
www domain = testdomain
```

www downlink

This command allows you to define rule expressions to match downlink (network to subscriber) HTTP/WSP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] www downlink *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match downlink HTTP/WSP packets.

Example

The following command defines a rule expression to match all downlink WWW packets:

```
www downlink = TRUE
```

www first-request-packet

This command allows you to define rule expressions to match the GET or POST request, if it is the first WSP/HTTP request for the subscriber's session.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] www first-request-packet *operator condition*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **FALSE**
- **TRUE**

Usage

Use this command to define rule expressions to match the GET or POST request, if it is the first WSP/HTTP request for the subscriber's session.

Example

The following command defines a rule expression to match user traffic based on the WWW first-request-packet:

```
www first-request-packet = TRUE
```

www header-length

This command allows you to define rule expressions to match WWW packet header length.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] www header-length *operator header_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

header_length

Specifies the WWW packet header length (in bytes) to match, *header_length* must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match WWW packet header length.

Example

The following command defines a rule expression to match user traffic based on WWW packet header length of *10000* bytes:

```
www header-length = 10000
```

www host

This command allows you to define rule expressions to match the “host name” header field present in HTTP/WSP headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] www host [case-sensitive] *operator host_name*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

host_name

Specifies the WWW host name to match.
host_name must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the host name header field present in HTTP/WSP headers.

Example

The following command defines a rule expression to match user traffic based on WWW host name *host1*:

```
www host = host1
```

www payload-length

This command allows you to define rule expressions to match WWW payload length.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] www payload-length *operator payload_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

payload_length

Specifies the payload length (in bytes) to match.
payload_length must be an integer from 1 through 4000000000.

Usage

Use this command to define rule expressions to match WWW payload length.

Example

The following command defines a rule expression to match user traffic based on WWW payload length of *10000*:

```
www payload-length = 10000
```

www pdu-length

This command allows you to define rule expressions to match WWW PDU length.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] www pdu-length *operator pdu_length*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

pdu_length

Specifies the WWW PDU length (in bytes) to match.
pdu_length must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match WWW PDU length (header + payload) in bytes.

Example

The following command defines a rule expression to match user traffic based on WWW PDU length of *9767* bytes:

```
www pdu-length = 9767
```

www previous-state

This command allows you to define rule expressions to match previous HTTP/WSP(HTTP) state.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] www previous-state *operator www_previous_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

www_previous_state

Specifies the previous state to match.
www_previous_state must be one of the following:

- **init**
- **response-error**
- **response-ok**
- **waiting-for-response**

Usage

Use this command to define rule expressions to match a previous HTTP/WSP(HTTP) state.

Example

The following command defines a rule expression to match user traffic based on WWW previous state **init**:

```
www previous-state = init
```

www reply code

This command allows you to define rule expressions to match WWW reply code arguments.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] www reply code *operator reply_code*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

reply_code

Specifies the reply code to match.
reply_code must be an integer from 100 through 599.

Usage

Use this command to define rule expressions to match HTTP 1.1 status code, or WSP status code that has been remapped to the corresponding HTTP value.
WSP status codes 0 – 101 are automatically remapped to the HTTP status code values, as defined by Table 36 WAP-230-WSP Version 5.

Example

The following command defines a rule expression to analyze WWW user traffic based on reply code of *125*:

```
www reply code = 125
```

www state

This command allows you to define rule expressions to match current HTTP/WSP(HTTP) state.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] www state *operator current_state*

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

current_state

Specifies the current state to match.
current_state must be one of the following:

- **close**
- **response-error**
- **response-ok**
- **waiting-for-response**

Usage

Use this command to define rule expressions to match current HTTP/WSP state.

Example

The following command defines a rule expression to match user traffic based on the current WWW state **close**:

```
www state = close
```

www transfer-encoding

This command allows you to define rule expressions to match the transfer encoding field present in HTTP/WSP(HTTP) headers.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] www transfer-encoding [case-sensitive] *operator transfer_encoding*

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

transfer_encoding

Specifies the WWW transfer encoding to match.
transfer_encoding must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the “transfer encoding” field present in HTTP/WSP(HTTP) headers.

Example

The following command defines a rule expression to match user traffic based on the WWW transfer encoding *user1*:

```
www transfer-encoding = user1
```

www url

This command allows you to define rule expressions to match URL for any Web protocol analyzer—HTTP, WAP1.X, WAP2.0.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[no] www url [case-sensitive] *operator url*

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

---

operator

Specifies how to match.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

---

url

Specifies the URL to match.
url must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the URL for any Web protocol analyzer—HTTP, WAP1.X, WAP2.0.

Example

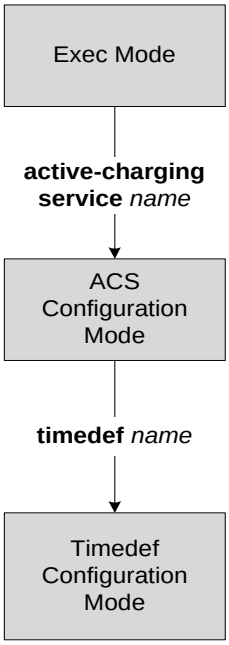
The following command defines a rule expression to match user traffic based on WWW URL *www.abc.com*:

```
www url = www.abc.com
```

Chapter 18
ACS Timedef Configuration Mode Commands

The ACS Timedef Configuration Mode enables configuring the Time-of-Day Activation/Deactivation feature.

Important: This configuration mode is only available in StarOS 8.1 and in StarOS 9.0 and later releases.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

start

This command allows you to configure timeslots in the current timedef.

Important: This command is only available in StarOS 8.1 and in StarOS 9.0 and later releases.

Important: A maximum of 24 timeslots can be specified within a timedef.

Product

All

Privilege

Security Administrator, Administrator

Syntax

`[ no ] start day { friday | monday | saturday | sunday | thursday | tuesday | wednesday } time` *`hh mm ss`* **`end day { friday | monday | saturday | sunday | thursday | tuesday | wednesday } time`** *`hh mm ss`*

`[ no ] start time` *`hh mm ss`* **`end time`** *`hh mm ss`*

`no`

If previously configured, removes the specified timeslot from the current timedef.

`start day { friday | monday | saturday | sunday | thursday | tuesday | wednesday } time` *`hh mm ss`* **`end day { friday | monday | saturday | sunday | thursday | tuesday | wednesday } time`** *`hh mm ss`*

Specifies a timeslot with a start day and time, and an end day and time.

- **`start day`**: Specifies the start day and start time.
- **`end day`**: Specifies the end day and end time.
- **`time`** *`hh mm ss`*: Specifies the start/end time:
  - *`hh`*: Specifies the start/end hour, and must be an integer from 0 through 23.
  - *`mm`*: Specifies the start/end minute, and must be an integer from 0 through 59.
  - *`ss`*: Specifies the start/end second, and must be an integer from 0 through 59.

`start time` *`hh mm ss`* **`end time`** *`hh mm ss`*

Specifies a timeslot with a start time and an end time to be applicable for all days of the week.
In specifying the start/end time:

- *`hh`*: Specifies the start/end hour, and must be an integer from 0 through 23.
- *`mm`*: Specifies the start/end minute, and must be an integer from 0 through 59.
- *`ss`*: Specifies the start/end second, and must be an integer from 0 through 59.

Usage

Use this command to create timeslots in a timedef during which rules have to be active. Timedefs enable activation/deactivation of ruledefs/groups-of-ruledefs such that they are available for rule matching only when they are active.
When a packet is received, and a ruledef/group-of-ruledefs is eligible for rule matching, if a timedef is associated with the ruledef/group-of-ruledefs, before rule matching, the packet-arrival time is compared with the timeslots configured in the timedef. If the packet arrived in any of the timeslots configured in the associated timedef, rule matching is undertaken, else the next ruledef/group-of-ruledefs is considered.

Important: The time considered for timedef matching is the system's local time.

This release does not support configuring a timeslot for a specific date.
If in a timeslot, only the time is specified that timeslot will be applicable for all days.
If for a timeslot "start time" is after "end time", that rule will span midnight and be considered to be active from the current day until the next day.
If for a timeslot, "start day" is after "end day", that rule will span the current week until the end day in the next week.
In the following cases a rule will be active all the time:

- A timedef is not configured in an action priority
- A timedef is configured in an action priority, but the named timedef is not defined
- A timedef is defined but without timeslots

Example

The following command specifies a timeslot that starts on *Tuesday* at *09:00:00* and ends on *Friday* at *21:30:00*:

```
start day tuesday time 9 0 0 end day friday time 21 30 0
```

The following command specifies a timeslot that starts at *15:00:00* and ends at *17:00:00* on all days of the week:

```
start time 15 0 0 end time 17 0 0
```

The following command specifies a timeslot that starts on *Friday* at *22:00:00* and ends on *Tuesday* at *08:00:00*. This timeslot spans the complete week until the end day, up to *Tuesday*.

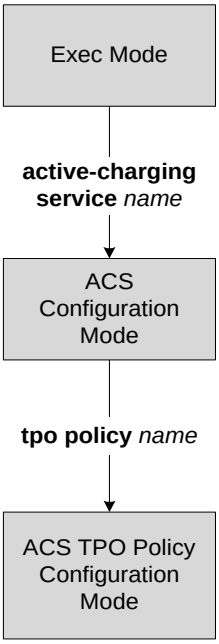
```
start day friday time 22 0 0 end day tuesday time 8 0 0
```

The following command specifies a timeslot that starts at *16:00:00* and ends at *09:00:00* on all days of the week. Also, as start time > end time, this timeslot spans midnight too (that is, from *16:00:00* to *23:59:59* and from *00:00:00* to *09:00:00*).

```
start time 16 0 0 end time 9 0 0
```

Chapter 19
ACS TPO Policy Configuration Mode Commands

The ACS TPO Policy Configuration Mode is used to configure Traffic Performance Optimization (TPO) policies.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

ad-filter

This command allows you to configure the bypass string for the Advertisement Filter feature.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

ad-filter ad-click-identity *bypass_string*

no ad-filter ad-click-identity

no

Removes the bypass string if previously configured.

bypass_string

Specifies the bypass string.
bypass_string must be an alphabetic string of 1 through 14 characters.

Important: The bypass string must consist of any of the following characters: "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ". Numeric and special characters are not accepted.

Usage

Use this command to configure the bypass string for the Advertisement Blocking with On-click feature. To enable retrieving a blocked advertisement requested by the subscriber, in the HTTP request the bypass string is added to the advertisement's URL, which TPO interprets and forwards to the Web Server allowing the advertisement to be retrieved.

Example

The following command configures the bypass string as *allow*:

```
ad-filter ad-click-identity allow
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

match-ad

This command allows you to define rules to match advertisements.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

match-ad priority *rule_priority* **tpo-ruledef** *tpo_ruledef_name*

no match-ad priority *rule_priority*

no

If previously configured, removes the specified TPO match-advertisement rule from the current TPO policy.

priority *rule_priority*

Specifies the priority of the TPO match-advertisement rule in the current TPO policy.
rule_priority must be an integer from1 through 65535, and must be unique in the current TPO policy.

tpo-ruledef *tpo_ruledef_name*

Specifies the TPO rule to add/remove from the current TPO policy.
tpo_ruledef_name must be the name of a TPO ruledef, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define the rules to block advertisements.

Example

The following command creates a match-advertisement rule to use the TPO ruledef named *tporule1* with the priority *1*:

```
match-ad priority 1 tpo-ruledef tporule1
```

match-rule no-ruledef-match

This command allows you to specify the action to be taken when the traffic does not match any TPO ruledef.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

match-rule no-ruledef-match tpo { none | profile *tpo_profile_name* **}**

default match-rule no-ruledef-match

default

Configures this command with its default setting.
Default: **none**. No TPO profile is selected.

none

Specifies that no TPO profile be used.

profile *tpo_profile_name*

Specifies the TPO profile to use when there is no rule match.
tpo_profile_name must be the name of a TPO profile, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify the action to be taken when the traffic does not match any TPO ruledef in the TPO policy.

Example

The following command specifies to use a TPO profile named *tpo_profile2* when the traffic does not match any TPO ruledefs in the TPO policy:

```
match-rule no-ruledef-match tpo profile tpo_profile2
```

match-rule priority

This command allows you to specify the TPO profile to use when the traffic matches a particular TPO ruledef/TPO group-of-ruledefs.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

match-rule priority *rule_priority* **{ tpo-group-of-ruledefs** *tpo_group_of_ruledefs_name* **| tpo-ruledef** *tpo_ruledef_name* **} tpo { none | profile** *tpo_profile_name* **} [description** *description* **]**

no match-rule priority *rule_priority*

no

Removes the specified match rule configuration.

match-rule priority *rule_priority*

Specifies priority of the rule within the TPO policy.
rule_priority must be an integer from1 through 65535, and must be unique in the current TPO policy.

tpo-group-of-ruledefs *tpo_group_of_ruledefs_name*

Important: The **tpo-group-of-ruledefs** option is available only in 12.2 and later releases.

Specifies the TPO group-of-ruledefs.
tpo_group_of_ruledefs_name must be the name of the TPO group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.
If any of the ruledefs within a group-of-ruledefs match, that group-of-ruledefs is considered a match.

tpo-ruledef *tpo_ruledef_name*

Specifies the TPO rule.
tpo_ruledef_name must be the name of a TPO ruledef, and must be an alphanumeric string of 1 through 63 characters.

tpo { none | profile *tpo_profile_name* **}**

Specifies the TPO profile to be used.

- **none**: Specifies that no TPO profile be used.
- **profile** *tpo_profile_name*: Specifies the TPO profile to be used. *tpo_profile_name* must be the name of a TPO profile, and must be an alphanumeric string of 1 through 63 characters.

description *description*

Adds the specified description to this rule priority configuration.

description must be an alphanumeric string of 1 through 127 characters.

Usage

Important: A maximum of 2048 optimization rules can be configured in the system.

Use this command to specify the TPO profile to use when the traffic matches a particular TPO ruledef/TPO group-of-ruledefs in the TPO policy.
This CLI command can be entered multiple times to specify multiple rules and TPO profiles. The rules are examined in order of priority, until a match is found and the corresponding TPO profile is applied. Lower numbered priorities are examined first.

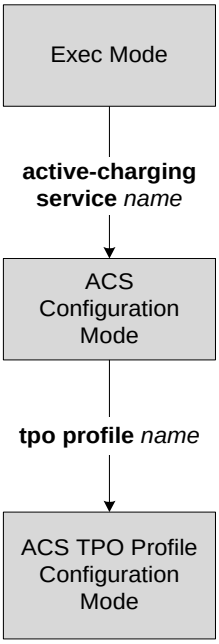
Example

The following command creates a rule match configuration to use the TPO profile named *tpoprofile1* when the traffic matches the TPO ruledef named *tporule1* with priority *1*:

```
match-rule priority 1 tpo-ruledef tporule1 tpo profile tpoprofile1
```

Chapter 20
ACS TPO Profile Configuration Mode Commands

The ACS TPO Profile Configuration Mode is used to configure Traffic Performance Optimization (TPO) profiles.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

http

This command allows you to configure the HTTP parameters.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

http { ad-filter display { no-text | text-only *text_only_string* **| text-with-click** *text_with_click_string* **} | compression | optimize-compressed-page | params { ad-filter display bgcolor** *bg_color_code* **| compression level** *compression_level* **| url-rewrite prefix** *url_rewrite_prefix* **} | prevent-server-compression | url-rewrite }**

default http { ad-filter display | compression | optimize-compressed-page | params { ad-filter display bgcolor | compression level | url-rewrite prefix } | prevent-server-compression | url-rewrite }

no http { compression | optimize-compressed-page | params ad-filter display bgcolor | prevent-server-compression | url-rewrite }

---

default

Configures this command with the default setting for the specified parameter.
Default:

- **ad-filter display**: none
- **compression**: Disabled
- **optimize-compressed-page**: Disabled
- **params**:
  - **ad-filter display bgcolor**: FFFFFF
  - **compression level**: 6
  - **url-rewrite prefix**: urlrewrite
- **prevent-server-compression**: Disabled
- **url-rewrite**: Disabled

---

no

Deletes TPO configuration for the specified parameter.

---

ad-filter display { no-text | text-only *text_only_string* **| text-with-click** *text_with_click_string* **}**

Enables HTTP Advertisement Filter, and configures the specified options:

- **no-text**: Blocks advertisements. Mobile client users see the “cannot display image” icon (usually an X mark) instead of a blocked advertisement. Users cannot view the blocked advertisements even if they want to.

- **text-only** *text_only_string*: Blocks advertisements. Mobile client users will see a placeholder frame instead of each blocked advertisement. Each placeholder frame contains the text specified here along with the advertisement's URL. Users cannot view the blocked advertisements even if they want to.

  text_only_string must be an alphanumeric string of 1 through 255 characters.

- **text-with-click** *text_with_click_string*: Blocks advertisements. Mobile client users will see a placeholder frame instead of each blocked advertisement. Each placeholder frame contains the text specified here along with the advertisement's URL. To view the blocked advertisements, users must click the placeholder frames.

  text_with_click_string must be an alphanumeric string of 1 through 255 characters.

---

compression

Enables HTTP compression for Web pages.
Default: Disabled

---

optimize-compressed-page

Enables uncompressing of compressed Web pages to apply other HTTP optimization techniques.
If the Web server responds to the mobile client with a compressed Web page, in order to apply other HTTP optimization techniques that maybe enabled, TPO can uncompress the Web page, apply the other HTTP optimizations, recompress the Web page, and then send it to the mobile client.
Default: Disabled

---

params { ad-filter display bgcolor *bg_color_code* **| compression level** *compression_level* **| url-rewrite prefix** *url_rewrite_prefix* **}**

Configures HTTP compression optimization parameters:

- **ad-filter display bgcolor** *bg_color_code*: For the HTTP Advertisement Filter feature, specifies color code for the advertisement placeholder frames' background.

  bg_color_code must be a string of 1 through 6 hexadecimal characters.

- **compression level** *compression_level*: Enables HTTP compression, and specifies the compression level.

  compression_level specifies the HTTP compression level, and must be an integer from 1 through 9. The higher the compression level, the better the compression but with a higher CPU and memory utilization.

  Default: 6

- **url-rewrite prefix** *url_rewrite_prefix*: Enables HTTP URL rewrite, and specifies the HTTP URL rewrite prefix.

  url_rewrite_prefix specifies the HTTP URL rewrite prefix, and must be an alphanumeric string of 8 through 32 characters.

  When embedded URLs are returned, they are replaced. For example, when "http://www.foo.com/xxx" is in the response, the URL is replaced with "http://ip-address/<url_rewrite_prefix>/www.foo.com/xxx". In this example, the DNS client resolves "www.foo.com" and puts that resolution as "ip-address". When the subscriber later does a GET, that request is modified as:

  URL: STRING/www.foo.com/xxx — will be changed to be just xxx

  Host: ip-address — will be changed to be "www.foo.com"

Default: urlrewrite

prevent-server-compression

Specifies TPO (to manipulate the HTTP request) to prevent server compression at the Web server.
TPO receives uncompressed data from the Web server, on which it can apply other HTTP optimization techniques, and then compresses and sends the data to the mobile client.
Default: Disabled

url-rewrite

Enables the URL Rewrite feature.
The URLs that are embedded in response pages are rewritten. This eliminates the need for the subscriber to perform DNS to resolve those URLs. See the **url-rewrite** option.
Default: Disabled

Usage

Use this command to configure TPO's HTTP parameters.

Example

The following command configures HTTP compression optimization parameter to level *3*:

```
http params compression level 3
```

p2p-detected

This command allows you to disable/continue TPO optimizations when a P2P flow is detected.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

```
p2p-detected { cease-tpo | continue-tpo }

default p2p-detected
```

default

Configures this command with its default setting.
Default: **continue-tpo**

cease-tpo

Specifies to disable TPO optimizations when a flow is detected as P2P.

Important: In this release, only TPO TCP optimizations are disabled. Disabling HTTP optimizations will be supported in a future release.

continue-tpo

Specifies to continue TPO optimizations when a flow is detected as P2P.

Usage

Use this command to disable/continue TPO optimizations when a P2P flow is detected.
While switching TPO profiles, if P2P flow is detected, TPO optimizations will be ceased/allowed based on the current TPO profile's configuration.

Example

The following command disables all TPO TCP optimizations when a P2P flow is detected:

```
p2p-detected cease-tpo
```

tcp

This command allows you to configure the TCP parameters.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

tcp { bandwidth { *bandwidth_kbps* | dynamic } | buffer-size { downlink | uplink } *buffer_size_kb* | congestion-control { basic | vegas | westwood-plus } | fast-retransmit-dupacks { *duplicate_acks* | dynamic } | handoff-optimization | initial-window { *initial_window* | dynamic bdp-percent *bdp_percent* | rfc5681 } | mss *mss* | pacing | rto { retrans-backoff { 1.0 | 1.5 | 2.0 } | rttvar-scaling *scaling_factor* } }

default tcp { bandwidth | buffer-size { downlink | uplink } | congestion-control | fast-retransmit-dupacks | handoff-optimization | initial-window | mss | pacing | rto { retrans-backoff | rttvar-scaling } }

no tcp { bandwidth | handoff-optimization | pacing }

---

no

Removes/disables the specified configuration.

---

default

Configures this command with the default setting for the specified parameter.
Default:

- **bandwidth**: No known bandwidth limit
- **buffer-size**:
  - **downlink**: 128 KB
  - **uplink**: 32 KB
- **congestion-control**: basic
- **fast-retransmit-dupacks**: 3
- **handoff-optimization**: Disabled
- **initial-window**: rfc5681
- **mss**: 536 bytes
- **pacing**: Disabled
- **rto**:
  - **retrans-backoff**: 2.0
  - **rttvar-scaling**: 2

bandwidth { *bandwidth_kbps* | dynamic }

Specifies bandwidth, which is used by TCP to optimize the data transfer rate.

- *bandwidth_kbps* specifies the maximum available bandwidth for a TCP flow, in kbps, and must be an integer from 1 through 100000.
- **dynamic** specifies the use of a value that is computed dynamically at runtime.

Default: No known bandwidth limit, same as **no tcp bandwidth** command.

buffer-size { downlink | uplink } *buffer_size_kb*

Specifies the socket send and receive buffer size for uplink/downlink traffic.

- **downlink**: Specifies the maximum amount of data that can be buffered inside TCP Proxy in downlink direction for each TCP connection. When the amount of data buffered in TCP Proxy in downlink direction reaches this limit, TCP Proxy sets receive window size in TCP header to 0 towards TCP server.
- **uplink**: Specifies the maximum amount of data that can be buffered inside TCP Proxy in uplink direction for each TCP connection. When the amount of data buffered in TCP Proxy in uplink direction reaches this limit, TCP Proxy sets receive window size in TCP header to 0 towards TCP client.

buffer_size_kb specifies the buffer size, in kilobytes, an must be an integer from 4 through 8192.

congestion-control { basic | vegas | westwood-plus }

Specifies the TCP congestion-control algorithm to use.

- **basic**: Use the basic TCP congestion-control algorithm.
- **vegas**: Use the Vegas TCP congestion-control algorithm.
- **westwood-plus**: Use the Westwood-plus TCP congestion-control algorithm.

Default: **basic**

fast-retransmit-dupacks { *duplicate_acks* | dynamic }

Specifies the number of duplicate ACKs required for fast retransmission.

- *duplicate_acks*: Specifies the number of duplicate ACKs that will trigger a fast-retransmit of the missing segment. After the specified number of duplicate ACKs is received, it is assumed that the segment was lost and is retransmitted.

  duplicate_acks must be an integer from 1 through 10. Default: 3

- **dynamic**:

  In 12.0 and earlier releases, this keyword dynamically changes the number of duplicate ACKs required for fast retransmission based on the number of in-flight packets (one-third of the in-flight packets, subject to a minimum of two). This helps to eliminate spurious retransmissions when packet reordering in the network is high.

In 12.2 and later releases, this keyword dynamically changes the number of duplicate ACKs required for fast retransmission based on the number of in-flight packets, and controls the actions taken on D-SACK detection. If the **dynamic** keyword is not configured, D-SACK detection takes place, but no action is taken.

Important: If the client does not support SACK, the behavior falls back to the behavior as described for earlier releases.

For information on D-SACK Support, refer to the *Traffic Performance Optimization Administration Guide*.

handoff-optimization

Enables handoff detection and relevant processing by TCP.
Default: Disabled

initial-window { *initial_window* | dynamic bdp-percent *bdp_percent* | rfc5681 }

Specifies the initial window size for a TCP session.

- *initial_window*: Specifies the initial-window as Maximum Segment Size (MSS), and must be an integer from 1 through 255.
- **dynamic bdp-percent** *bdp_percent*: Use a dynamically computed value at runtime, that is calculated as a percentage of bandwidth-delay product (BDP).

  bdp_percent must be an integer from 1 through 100.

  Bandwidth information is dynamically derived from the **bandwidth** command. The delay is calculated using the SYN-ACK exchange. If bandwidth information is not available, this configuration has no effect (behavior will be same as the default setting).
- **rfc5681**: Use a value recommended by RFC 5681, which will vary from 2 through 4 based on MSS.

Default: **rfc5681**

mss *mss*

Specifies the Maximum Segment Size (MSS), in bytes.
mss must be an integer from 248 through 65535.
Default: 536 bytes

pacing

Enables TCP Pacing.
Under some conditions (typically at the end of fast-recovery) a single ACK is received, which acknowledges huge amounts of data. Because of this, the sliding-window suddenly shifts to the right, causing the sender to burst huge amount of data into the network at one shot; this typically triggers a tail-drop (loss of series of packets) at the bottleneck router. Huge data bursts can also occur due to other factors, such as ACK compression. TCP Pacing causes the sender to evenly distribute the window of data over an entire round-trip time (RTT).
Default: Disabled

rto { retrans-backoff { 1.0 | 1.5 | 2.0 } | rttvar-scaling *scaling_factor* **}**

Specifies Retransmission Timeout (RTO) settings.

- **retrans-backoff { 1.0 | 1.5 | 2.0 }**

  Specifies the RTO back-off factor. Once retransmission timeout RTO fires for a packet, TCP will retransmit that packet and set the RTO to be a factor X, specified here, of the previous RTO.

  Default: 2.0

  - **1.0**: Use backoff factor 1.0.
  - **1.5**: Use backoff factor 1.5.
  - **2.0**: Use backoff factor 2.0.
- **rttvar-scaling** *scaling_factor*

Specifies the scaling factor for Round Trip Time Variation (RTTVAR).

The configured scaling factor is used as a power of 2, so values of 0 through 4 correspond to 1, 2, 4, 8, and 16. RTO is calculated in TCP using following formula:

RTO = SRTT + K*RTTVAR

where:

- SRTT = mean Round Trip Time (RTT)
- RTTVAR = Round Trip Time Variation

As wireless networks exhibit high RTT variation, the value of K is made configurable. The value of K decides the extent to which RTO timer depends on RTT variance. If RTT variance is higher, then K should be higher.

scaling_factor must be an integer from 0 through 4.

Default: 2

Usage

Use this command to configure TPO TCP parameters.

Example

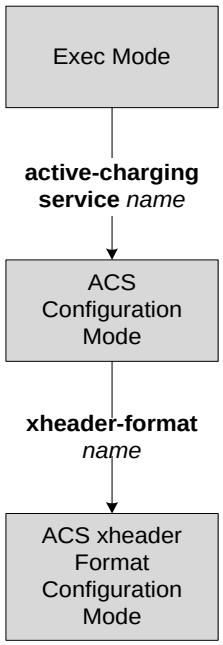
The following command configures the initial window size for a TCP session to *100*:

```
tcp initial-window 100
```

Chapter 21
ACS x-header Format Configuration Mode Commands

The ACS x-header Format Configuration Mode is used to create and configure extension-header (x-header) formats.

Important: This feature is license dependent. Please contact your Cisco sales representative for more information.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

insert

This command allows you to configure the x-header fields to be inserted in HTTP/WSP GET and POST request packets.

Important: This command is license dependent. Please contact your Cisco accounts representative for more information.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

In StarOS 8.0:

insert *xheader_field_name* **{ string-constant** *xheader_field_value* **| variable { bearer { 3gpp charging-id | ggsn-address | imsi | radius-calling-station-id | sgsn-address | sn-rulebase | subscriber-ip-address } | http { host | url } }**

no insert *xheader_field_name*

In StarOS 8.1, StarOS 9.0, and later releases:

insert *xheader_field_name* **{ string-constant** *xheader_field_value* **| variable { bearer { 3gpp { apn | charging-characteristics | charging-id | imei | imsi | qos | rat-type | s-mcc-mnc | sgsn-address } | acr | customer-id | ggsn-address | mdn | msisdn-no-cc | radius-calling-station-id | session-id | sn-rulebase | subscriber-ip-address | username } [encrypt] | http { host | url } }**

no insert *xheader_field_name*

no

If previously configured, removes the specified x-header field configuration.

xheader_field_name

Specifies the x-header field name to be inserted in the packets.
xheader_field_name must be an alphanumeric string of 1 through 31 characters.
Up to ten fields can be inserted in each x-header format.

string-constant *xheader_field_value*

Specifies constant a string value for x-header field to be inserted in the packets.
xheader_field_value must be the x-header field value, and must be an alphanumeric string of 1 through 63 characters.

variable

Specifies name of the x-header field whose value must be inserted in the packets.

bearer { 3gpp { apn | charging-characteristics | charging-id | imei | imsi | qos | rat-type | s-mcc-mnc | sgsn-address } | acr | customer-id | ggsn-address | mdn | msisdn-no-cc | radius-calling-station-id | session-id | sn-rulebase | subscriber-ip-address | username } [encrypt]

Specifies value of x-header field to be inserted:

- **3gpp**: 3GPP service.
  - **apn**: APN of the bearer flow. This field is deprecated from under **bearer apn** and has been added within **bearer 3gpp apn**.
  - **charging-characteristics**: Charging characteristics of the bearer flow.
  - **charging-id**: Charging ID of the bearer flow.
  - **imei**: IMEI or IMEISV (depending on the case) associated with the bearer flow.
  - **imsi**: Specific Mobile Station Identification number.
  - **qos**: EPC QoS associated with the bearer flow.

    The inserted x-header is seen as:

    x-bearer-qos: 020400000100000002000000010000000200\r\n
  - **rat-type**: This field is deprecated from under **bearer rat-type** and has been added within **bearer 3gpp rat-type**.
  - **s-mcc-mnc**: 3GPP serving node MCC + MNC associated with the bearer.

    The inserted x-header is seen as: x-s-mcc-mnc: 123765\r\n
  - **sgsn-address**: SGSN associated with the bearer flow.
- **acr**: Anonymous Customer Reference. Only MSISDN part of this is encrypted, if encrypt flag is set.
- **customer-id**: Customer ID of the bearer.
- **ggsn-address**: GGSN IP address field.
- **imsi**: This field is deprecated from within **bearer imsi** and has been moved within **bearer 3gpp imsi**. The IMSI as added via **bearer 3gpp imsi**.
- **mdn**: MDN of the bearer flow.
- **msisdn-no-cc**: MSISDN of the mobile handling the flow without the country code.
- **radius-calling-station-id**: Calling Station ID of the mobile handling the flow. Use this for MSISDN of the mobile handling the flow with the country code.
- **session-id**: Accounting session ID of the bearer flow.
- **sn-rulebase**: Name of the ACS rulebase.
- **sgsn-address**: This field is deprecated from under **bearer sgsn-address** and has been moved within **bearer 3gpp sgsn-address**.
- **subscriber-ip-address**: Subscriber IP address.
- **username**: User name of the bearer flow.

encrypt: Specifies encryption of x-header field configuration. This option must only be configured when x-header encryption is enabled.

http { host | url }

Specifies value of the x-header field to be inserted:

- **host**: Host

- **url**: Uniform Resource Locator

Usage

Use this command to configure the x-header fields to be inserted in HTTP/WSP GET and POST request packets. The x-headers would be inserted at the end of the HTTP/WSP header. This CLI command may be used up to 10 times. There is no control over the order of the fields that are to be inserted. Any of the indicated ruledef variables may be inserted using the variable option, or a static string may be inserted using the string-constant option.
Operators may insert x-headers in some HTTP/WSP packets, for which some rules will be configured. The charging-action associated with these rules will contain the list of x-headers to be inserted in the packets.

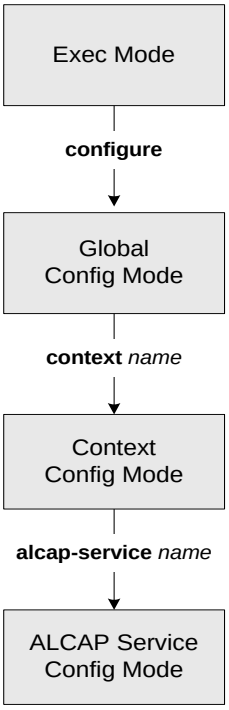
Example

The following command configures an x-header field named *test12* with a constant string value of *testing* to be inserted in HTTP/WSP GET and POST request packets:

```
insert test12 string-constant testing
```

Chapter 22
ALCAP Configuration Mode Commands

The ALCAP Service Configuration Mode is used to create, provide, and manage the Access Link Control Application Part (ALCAP) on HNB-GW to support IuCS-over-ATM connectivity to HNB subscriber in a 3G UMTS networks towards CS core network.



aal2-node

Thsi command creates/configures AAL2 node configuration to defined AAL2 node properties for IuCS-over-ATM fucntion.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

aal2-node *aal2_node_name* [**-noconfirm**]

no aal2-node *aal2_ndoe_name*

no

Removes the configured AAL2 node from ALCAP service configuration.

aal2_node_name

Identifies the name of the AAL2 node name to configure the AAL2 node paramters.
The *aal2_node_name* must be an alphanumerical string from 1 through 63 characters.

Usage

Use this command to create/configure the AAL2 node configuration and switch to AAL2 Node Configuration mode.
Entering this command results in the following prompt:
`[context_name]hostname(config-aal2-node-aal2_node_name)#`
A maximum of *TBD* AAL2 node can be configured in one ALCAP service.

Important: The AAL2 Node configured here will be used to bind with ATM port in PVC Configuration sub-mode of ATM Configuration mode for IuCS-over-ATM functionality.

Important: For more information on AAL2 node configuration, refer *AAL2 Node Configuration Mode Commands*.

Example

Following command creates AAL2 node configuration mode named *aal2_1* within the specific ALCAP service for IuCS-over-ATM support towards CS core networks and switch the user to AAL2 Node Configuration Mode named *aal2_1*:

aal2-node *aal2_node_name* **-noconfirm**

aal2-route

This command defines a route for each ATM Endpoint Service Address (AESA) with which it can have transport layer communication. This route actually maps an AESA to one or more AAL2 paths which will be used to setup an end to end communication path.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

aal2-route end-point {*AESA_address* | **default**} **aal2-node** *aal2_node_name*

no aal2-route end-point {*AESA_address* | **default**} [**aal2-node** *aal2_node_name*]

no

Removes defined AAL2 route from ALCAP service configuration.

end-point [*AESA_address* **| default]**

Specifies the AESA address in an ATM (or AAL2) network to map with adjacent AAL2 node. The AESA is based on the generic network service access point (NSAP) format. The ATM connection from HNB-GW terminates at this point.
The *AESA_address* must be an alpha/numeric string from 1 through 63 characters.
The **default** keyword is used to configure a default AAL2 route which will match any AESA received from MSC and for which AESA specific route is not configured. When a connection is established an AESA specific route will have higher priority than **default** route.

aal2-node *aal2_node_name*

Identifies the name of the AAL2 node name to configure in AAL2 route.
The *aal2_node_name* must be an alphanumerical string from 1 through 63 characters.

Usage

Use this command to create a mapping between ATM endpoint and adjacent node for AAL2 connection routing purposes.
It defines a route for each ATM Endpoint Service Address (AESA) with which it can have transport layer communication. This route actually maps an AESA to one or more AAL2 paths which will be used to setup an end to end communication path.
The **default** keyword can be used to configure a default **aal2-route** which will match any AESA received from MSC and for which AESA specific route is not configured. When a connection is established an AESA specific route will have higher priority than default route.

Important: The default route shall not be used when AESA specific route exists.

If an HNB-GW configured with a route for *MGW1* which consists of *AAL2_path_A* and *AAL2_path_B* for **AAL2 switch-A** and **AAL2 switch-B** switch respectively then similarly **AAL2 switch-A** and **AAL2 switch-B** need to be configured with routes for *MGW1*.

A maximum of *TBD* AAL2 routes can be configured in one ALCAP service.

Example

Following command create a mapping between ATM endpoint *MGW1* and AAL2 node *aal2_1* for AAL2 connection routing purposes:

```
aal2-route end-point MGW1 aal2-node aal2_1
```

associate

This command associates a previously configured SS7 routing domain with this ALCAP service on HNB-GW node which will be used to define the SS7 routing domain in 3G UMTS networks.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

associate ss7-routing-domain *ss7_rd_id*

no associate ss7-routing-domain

no

Removes the associated SS7 routing domain id from this ALCAP service configuration.

ss7_rd_id

Identifies the SS7 routing domain index configured in Global configuration mode to associate with ALCAP service for IuCS-over-ATM support.
The *ss7_rd_id* must be an integer from 1 through 12.

Important: For SS7 routing doman configuration, refer *SS7 Routing Domain Configuration Commands Mode* chapter.

Usage

Use this command to associate a preconfigured SS7 routing domain index to provide IuCS-over-ATM support towards CS core network for HNB subscriber.
A maximum of *TBD* SS7 routing domains can be configured in one ALCAP service.

Example

Following command associates a predefined SS7 routing domain id *3* with ALCAP service to define routing domain for IuCS-over-ATM supprot towards CS core networks:

```
associate ss7-routing-domain 3
```

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Return to the previous mode.

maximum reset-retransmission

This command sets the maximum number of retries allowed for transmission of RESET message to reset the AAL2 path.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

maximum reset-retransmissions *retries*

default maximum reset-retransmissions

default

Sets the number of RESET meesage retries to default value of 1.

retires

Sets the maximum number of retries allowed for transmission of RESET message to reset the AAL2 path by ALCAP service.
retries must be an integer value from 0 through 4. When 0 is used retransmission will be disabled.
Default: 1

Usage

Use this command to sets the maximum number of retries allowed for transmission of RESET message by ALCAP service to reset the AAL2 path when **Timer_RES** expires. Once the maximum number of RESET retries have been performed the ALCAP service shall stop the RESET procedure for the affected path and path will become available for connections.

Example

The following command configures ALCAP service to send maximum number of *2* RESET messages after expiry of RESET timer for AAL2 path RESET procedure:

```
maximum reset-retransmissions 2
```

self-point-code

This command specifies the SS7 point code address for ALCAP service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

self-point-code *point_code*

no self-point-code

no

Deletes the configured self point code for this ALCAP service.

point_code

Defines the point code to assign to this ALCAP service.
point_code: value entered must adhere to the point code variant selected when the ALCAP service instance was defined:

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- a string of 1 to 11 combined digits and period.

Usage

Use this command to assign the self point code to use for this ALCAP service.

Example

The following command sets an ITU-based point code for this ALCAP service:

```
self-pointcode 4.121.5
```

The following command removes the configured self-point code:

```
no self-pointcode
```

timeout alcap

This command configures the timeout duration for various ALCAP procedure timers in ALCAP service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

timeout alcap {**blo** *blo_timer_value* | **erq** *erq_timer_value* | **mod** *mod_timer_value* | **rel** *rel_timer_value* | **res** *res_timer_value* | **ubl** *ubl_timer_value*}

default timeout alcap {**blo** | **erq** | **mod** | **rel** | **res** | **ubl**}

default

Sets the timer values to default duration for specific ALCAP procedure in an ALCAP service.

blo *blo_timer_value*

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Path Block procedure. When a request to block a particular AAL2 path is recieved by ALCAP service, the ALCAP service sends ALCAP-BLOCK-REQEST message to AAL2 node/peer ALCAP Manage and starts **Timer_BLO** timer. The timer waits for specified timeout duration *blo_timer_value* for ALCAP-BLOCK-CONFRIM message before reporting error in procedure.
If AAL2 Node responds with ALCAP-BLOCK-CONFRIM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.
blo_timer_value must be an integer value from 2 through 60.
Default: 5

erq *erq_timer_value*

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Establish Request procedure. When a request to esblish a connection through ALCAP-ESTABLISH-REQUEST message is sent to AAL2 node the system starts the **Timer_ERQ** timer. The timer waits for specified timeout duration *erq_timer_value* for ALCAP-ESTABLISH-CONFRIM message before reporting error in procedure and system requests ALCAP Manager to free the AAL2-channel used for connection and also indicates to start the RESET procedure for this channel.
If AAL2 Node responds with ALCAP-ESTABLISH-CONFRIM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.
erq_timer_value must be an integer value from 5 through 30.
Default: 5

mod *mod_timer_value*

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Modify Request procedure. When a request to modify a connection or channel through ALCAP-MODIFY-REQUEST message is sent to AAL2 node the system starts the **Timer_MOD** timer. The timer waits for specified timeout duration *mod_timer_value* for ALCAP-MODIFY-CONFRIM message before reporting error in procedure and system requests ALCAP Manager to initiates the RESET or

any other appropriate procedure for this channel and HNB-GW shall release the RUA connection towards HNB and SCCP connection towards CN.
If AAL2 Node responds with ALCAP-MODIFY-CONFRIM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.
mod_timer_value must be an integer value from 5 through 30.
Default: 5

---

rel *rel_timer_value*

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Release Request procedure. When a request to release a connection or channel through ALCAP-RELEASE-REQUEST message is sent to AAL2 node the system starts the **Timer_REL** timer and sends RAB-ASST-REQ to HNB. The timer waits for specified timeout duration *rel_timer_value* for ALCAP-RELEASE-CONFRIM message before reporting error in procedure and system requests ALCAP Manager to release the AAL2 channel. System also indicates to start RESET procedure for this channel.
If AAL2 Node responds with ALCAP-RELEASE-CONFRIM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.
rel_timer_value must be an integer value from 2 through 60.
Default: 2

---

res *res_timer_value*

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Reset Request procedure. When a request to reset a connection or channel through ALCAP-RESET-REQUEST message is sent to AAL2 node the system starts the **Timer_RES** timer. The timer waits for specified timeout duration *res_timer_value* for ALCAP-RESET-CONFRIM message before retrying the RESET procedure. The system will retry the RESET procedure for configured number of times and on completion of retry limit the stops the RESET procedure for the affected path and path will become available for connections.
If AAL2 Node responds with ALCAP-RESET-CONFRIM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.
res_timer_value must be an integer value from 2 through 60.
Default: 2

---

ubl *ubl_timer_value*

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Path UnBlock procedure. When a request to unblock a particular AAL2 path is recieved by ALCAP service, the ALCAP service sends ALCAP-UNBLOCK-REQEST message to AAL2 node/peer ALCAP Manager and start **Timer_BLO** timer. The timer waits for specified timeout duration *ubl_timer_value* for ALCAP-UNBLOCK-CONFRIM message before reporting error in procedure.
If AAL2 node/peer ALCAP Manager responds with ALCAP-BLOCK-CONFRIM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.
ubl_timer_value must be an integer value from 2 through 60.
Default: 2

Usage

Use this command to configure the timeout duration for various ALCAP procedures in ALCAP service.

Example

The following command sets the timeout duration of 10 seconds for ALCAP-MODIFY-REQUEST procedure:

timeout alcap mod *10*

timeout stc

This command configures the timeout duration for STC long (T30) and and STC short (T29) timers used in congestion indication procedure at Signaling Transport Converter (STC) layer in ALCAP service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

timeout stc {**long** *long_timer_value* | **short** *short_timer_value*}

default timeout stc {**long** | **short**}

default

Sets the timer values to default duration for specific STC procedure in an ALCAP service.

long *long_timer_value*

Specifies the duration in millinseconds for STC long timer. This timer is used by the congestion indication procedure. Receipt of a repeated congestion indication from MTP3B before the expiry of this timer is interpreted as the congestion situation. On the other hand, if no congestion indication is received from MTP3B before expiry of this timer, the congestion situation is considered to have improved.
long_timer_value must be an integer value from 5000 through 10000.
Default: 5000

short *short_timer_value*

Specifies the duration in millinseconds for STC short timer. This timer is used by the congestion indication procedure. The role of this timer is to avoid overreacting if multiple congestion indications are received from MTP3B in quick succession.
short_timer_value must be an integer value from 300 through 600.
Default: 300

Usage

Use this command to configure the long (T30) and short (T29) timer for congestion indication procedure in ALCAP service.
When the first congestion indication is received by, the traffic load into the affected destination point code is reduced and the same time two timers STC short timer (T29) and STC long timer (T30) are started. During STC short timer all received congestion indications for the same destination point code are ignored in order not to reduce traffic too rapidly. Reception of a congestion indication after the expiry of STC short timer, but still during STC long timer, will decrease the traffic load by one more step and restart both the timers again. If STC long timer expires (i.e. no congestion indications having been received during the STC long timer period), traffic will be increased by one step and STC long timer will be restarted unless full traffic load has been resumed.

Example

The following command sets the timeout duration of 5000 milliseconds for STC long timer:

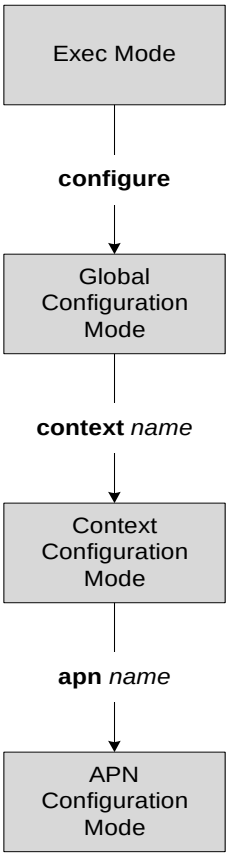
```
default timeout stc long
```

The following command sets the timeout duration of 300 milliseconds for STC short timer:

```
default timeout stc short
```

Chapter 23
APN Configuration Mode Commands

The Access Point Name (APN) Configuration Mode is used to create and configure APN profiles within the current system context of a UMTS/LTE service.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

aaa

This command configures Authentication, Authorization, and Accounting (AAA) functionality at the Access Point Name (APN) level.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

aaa { **group** *aaa_group_name* | **secondary-group** *aaa_group_name* }

default aaa { **group** | **secondary-group** *aaa_group_name* }

no aaa { **group** *aaa_group_name* | **secondary-group** }

no aaa

Disables the specified AAA group for the specific APN.

no aaa { group | secondary-group }

- **group**: Uses the default AAA group.
- **secondary-group**: Removes the secondary AAA group from the APN's configuration.

default aaa { group | secondary-group }

Configures the default setting for the specified parameter.

- **group**: Uses the default AAA group—the one specified at the context level or in the APN template.
- **secondary-group**: Removes the secondary AAA group from the APN configuration.

aaa_group_name

Specifies the AAA server group for the APN as an alphanumeric string of 1 through 63 characters.

secondary-group *aaa_group_name*

Specifies the secondary AAA server group for the APN. *aaa_group_name* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure AAA functionality at the APN level.
Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual server group for APNs in that context. Each server group consists of a list of AAA servers for each AAA function (accounting, authentication, charging, etc.).
The AAA secondary server group supports the RADIUS Fire-and-Forget feature in conjunction with GGSN for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting acknowledgement from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start / Interim / Stop) sent to the standard AAA RADIUS server.

If the same AAA group is configured with both the **aaa group** *aaa_group_name* and the **aaa secondary-group** *aaa_group_name* commands, then this configuration will have no effect and secondary accounting will not happen.
The AAA secondary server group configuration takes effect only when used with APN accounting-mode set to radius-diameter (or) with mediation-acct enabled. The RADIUS accounting triggers for both standard RADIUS accounting and secondary accounting will be taken from the AAA group configured with the **aaa group** *aaa_group_name* command. On the fly change of this configuration is not supported. Any change to the configuration will have effect only for new calls.

Example

The following command applies the AAA server group *star1* to an APN within the specific context:

```
aaa group star1
```

access-link

Configures IP fragmentation processing over the Access-link (PPP, GTP etc.).

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
access-link ip-fragmentation { normal | df-ignore | df-fragment-and-icmp-notify }

default access-link ip-fragmentation
```

normal

Default: Enabled
Drops the packet and sends an ICMP unreachable message to the source of packet. This is the default behavior.

df-ignore

Default: Disabled
Ignores the DF (Don’t Fragment) bit setting; fragments and forwards the packet over the access link.

df-fragment-and-icmp-notify

Default: Disabled
Partially ignorse the DF bit; fragments and forwards the packet, but also returns an ICMP error message to the source of the packet. The number of ICMP errors sent like this is rate-limited to one ICMP error packet per second per session.

Usage

If the IP packet to be forwarded is larger than the access-link MTU and if the DF (Don't Fragment) bit is set for the packet, then the fragmentation behavior configured by this command is applied. Use this command to fragment packets even if they are larger than the access-link MTU.
Fragmentation may also occur for other reasons, regardless of whether or not fragmentation is performed because of one of the above reasons.
Payloads are encapsulated within IP/UDP/GTP before being sent to the SGSN. If that encapsulation causes the packet to exceed 1500 bytes, the inner IP payload is fragmented (even if it's not considered too-large by the above tests) into two payloads (if the DF bit is not set). If the DF bit is set (and access-link ip-fragmentation normal is configured), the system performs IP fragmentation of the entire packet (i.e., IP fragmentation in the outer IP header) rather than fragmenting the inner IP payload. Either way, the result is two packets, but in one case the MS would have to perform IP reassembly while in the other case the SGSN would have to perform reassembly.

Example

Set fragmentation so that the DF bit is ignored and the packet is forwarded anyway by entering the following command:

```
access-link ip-fragmentation df-ignore
```

accounting-mode

Configures the protocol to be used for PDP context accounting by this APN.

Product

GGSN, ECS, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
accounting-mode { gtpp | none | radius-diameter [ no-interims ] [ no-early-pdus ] }

default accounting-mode
```

default

Restores the command to its default setting.

gtpp

Configures the APN to use GPRS Tunneling Protocol Prime for accounting purposes. If used, accounting will begin as soon as the PDP context is established. This is the default setting. Default: Enabled

Important: The system's GTPP parameters must be configured prior to using this protocol for accounting. Refer to the **gtpp** commands in the *Context Configuration Mode Commands* chapter.

none

Disables accounting for PDP contexts using this APN.
When accounting mode is set to none, it indicates to the GTP stack at session manager to not generate the regular GTPP accounting triggers. Default: Disabled.

radius-diameter

Configures the APN to use RADIUS/Diameter protocol for accounting purposes. Default: Disabled

Important: The system's RADIUS/Diameter accounting parameters must be configured prior to using either of the protocols for accounting. Refer to the **radius**/**diameter** commands in the *Context Configuration Mode Commands* and the *AAA Server Group Configuration Mode Commands* chapters.

no-early-pdus

Configures the GGSN to discard user traffic once the buffer is full until the RADIUS server has returned a response to the GGSN's accounting START request per 3GPP standards.
Configures the GGSN to delay PDUs from/to MS until the RADIUS server returns a response to the GGSN's accounting START request as per 3GPP standards. The GGSN buffers up to two PDUs per call. Additional PDUs disable the queuing. On receiving the Accounting response message, the GGSN forwards all the subsequent PDUs for that call.

Important: For StarOS 10.0 and earlier releases, the system buffers up to four PDUs and queues or discards the remaining PDUs.

Important: For StarOS 11.0 and later releases, the system is configured so that none of the PDUs are discarded.

no-interims

Disables the generation of RADIUS interims per APN.
When configured, RADIUS interim updates for this APN will not be sent, regardless of what is configured in the context that is used for RADIUS accounting.

Important: Different CLI commands are used to disable RADIUS interims for RADIUS accounting and mediation accounting. To disable RADIUS interims for RADIUS accounting, use the following command: **accounting-mode radius-diameter no-interims**. To disable RADIUS interims for mediation accounting, use the following command: **mediation-device context-name** *context_name* **no-interims**.

Usage

This command specifies which protocol, if any, will be used to provide accounting for PDP contexts accessing the APN profile.
When the GTPP protocol is used, accounting messages are sent to the charging gateways (CGs) over the Ga interface. The Ga interface and GTPP functionality are typically configured within the system's source context. As specified by the standards, a CDR is not generated when a session starts - CDRs are generated according to the interim triggers (configured using the **cc** command in the GGSN service configuration mode) and a CDR is generated when the session ends. For interim accounting, STOP/START pairs are sent based on configured triggers.
GTPP version 2 is always used. However, if version 2 is not supported by the CGF, the system reverts to using GTPP version 1. All subsequent CDRs are always fully-qualified partial CDRs. All CDR fields are R4.
If the **radius-diameter** option is used, either the RADIUS or the Diameter protocol is used as configured in the Context Configuration mode or the AAA Server Group Configuration mode.
If the RADIUS protocol is used, accounting messages can be sent over a AAA interface or the Gi to the RADIUS server. The AAA or Gi interface(s) and RADIUS functionality are typically configured with the system's destination context along with the APN. RADIUS accounting begins immediately after an IP address is allocated for the MS. Interim accounting can be configured using the **radius accounting interim interval**. The **radius accounting interim interval** command sends INTERIM-UPDATE messages at specific intervals.
Keywords to this command can be used in combination to each other, depending on configuration requirements.

Important: If the accounting type in the APN is set to 'none' then G-CDRs will not be generated. If accounting type is left as default "GTPP" and "billing-records" are configured in the ACS Rulebase Configuration Mode, then both G-CDRs and eG-CDRs would be generated.

Example

The following command configures the APN to use the RADIUS/Diameter protocol for accounting:

```
accounting-mode radius-diameter
```

```
accounting-mode radius-diameter no-interims no-early-pdus
```

```
accounting-mode radius-diameter no-early-pdus no-interims
```

active-charging bandwidth-policy

Configures the bandwidth policy to be used for subscribers who use this APN.

Product

GGSN, ECS

Privilege

Security Administrator, Administrator

Syntax

active-charging bandwidth-policy *bandwidth_policy_name*

[**default** | **no**] **active-charging bandwidth-policy**

default

Configures the default setting.
Default: The default bandwidth policy configured in the rulebase is used for subscribers who use this APN.

no

Disables bandwidth control for the APN.

bandwidth-policy *bandwidth_policy_name*

Specifies the bandwidth policy name. *bandwidth_policy_name* must be an alphanumeric string from 1 through 63 characters.

Usage

Use this command to configure bandwidth policy to be used for subscribers who use this APN.

Example

The following command configures a bandwidth policy named *standard* for the APN:

```
active-charging bandwidth-policy standard
```

active-charging link-monitor tcp

Enables the TCP link monitoring feature on the Mobile Video Gateway. This command can be configured in either APN Configuration Mode or Subscriber Configuration Mode.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] active-charging link-monitor tcp [ log [ rtt [ histogram | time-series ] [ bitrate [ histogram | time-series ] ] | bitrate [ histogram | time-series ] [ rtt [ histogram | time-series ] ] ] ] [ -noconfirm ]
```

default

Sets TCP link monitoring to its default value, which is the same as **no**.

no

Deletes the TCP link monitoring settings and disables TCP link monitoring if previously configured.

link-monitor tcp

Enables the TCP link monitoring feature on the Mobile Video Gateway. Note that TCP link monitoring is not enabled by default. Also note that when this command is configured without the **log** option, TCP link monitoring is enabled without logging, and the output from TCP link monitoring is only used by the dynamic translating feature.

log [rtt [histogram | time-series] [bitrate [histogram | time-series]] | bitrate [histogram | time-series] [rtt [histogram | time-series]]]

This option enables statistical logging for TCP link monitoring.
The **rtt** option can be used to enable either **histogram** or **time-series** logging for RTT.
Similarly, the **bitrate** option can be used to enable either **histogram** or **time-series** logging for bit rate.
When **rtt** and **bitrate** options are used without additional options, histogram and time-series logging are enabled for RTT and/or bit rate respectively.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to enable TCP link monitoring on the Mobile Video Gateway.

Examples

The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for both RTT and bit rate:

```
active-charging link-monitor tcp log
```

The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for RTT:

```
active-charging link-monitor tcp log rtt
```

The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT:

```
active-charging link-monitor tcp log rtt histogram
```

The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT and time-series logging enabled for bit rate:

```
active-charging link-monitor tcp log rtt histogram bitrate time-series
```

active-charging rulebase

Specifies the name of the Active Charging Service (ACS) rulebase to be used for subscribers who use this APN.

Product

GGSN, ECS, P-GW, MVG

Privilege

Security Administrator, Administrator

Syntax

active-charging rulebase *rulebase_name*

no active-charging rulebase

no

Removes the rulebase previously configured for this APN.

rulebase_name

Specifies the name of the ACS rulebase as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify the ACS rulebase to be used for subscribers who use the APN.

Example

The following command specifies the ACS rulebase named *rule1* for the APN:

```
active-charging rulebase rule1
```

apn-ambr

Configures the Aggregated Maximum Bit Rate (AMBR) for all PDNs using this APN.

Product

P-GW

Privilege

Administrator

Syntax

apn-ambr rate-limit direction { downlink | uplink } [burst-size { auto-readjust duration *seconds* **|** *bytes* **} | violate-action { drop | lower-ip-precedence | shape [transmit-when-buffer-full] | transmit }]**

[default | no] apn-ambr rate-limit direction { downlink | uplink }

default

Returns the selected command to it's default setting of no APN-AMBR.

no

Disables the selected command.

rate-limit direction { downlink | uplink }

Specifies that the rate limit is to be applied to either the downlink (network to subscriber) traffic or the uplink (subscriber to network) traffic.
downlink: Applies the AMBR parameters to the downlink direction.
uplink: Applies the AMBR parameters to the uplink direction.

burst-size { auto-readjust duration *seconds* **|** *bytes***}**

This parameter is used by policing and shaping algorithms to permit short bursts of traffic in order to not exceed the allowed data rates. It is the maximum size of the token bucket.
auto-readjust duration *seconds*: The duration (in seconds) used in this burst size calculation: burst size = peak data rate/8 * auto-readjust duration
seconds must be an integer value from 1 to 30. Default is 1 second
bytes: Specifies the burst size in bytes allowed by this APN for the associated PDNs. It must be an integer from 1 to 4294967295 (1 byte to 4 GB).

violate-action { drop | lower-ip-precedence | shape [transmit-when-buffer-full] | transmit }

The action that the P-GW will take when the data rate of the bearer context exceeds the AMBR.
drop: Drops violating packets.
lower-ip-precedence: Sets the DSCP value to zero ("best effort") for violating packets.
shape [transmit-when-buffer-full]: Places all violating packets into a buffer and, optionally, transmits the packets when the buffer is full.

Important: The **shape** keyword and optional **transmit-when-buffer-full** are only available in StarOS v12.0 and earlier releases. P-GW does not currently support traffic shaping for APN-AMBR.

transmit: Transmits violating packets. This is the default setting.

Usage

Use this command to enforce the AMBR for the APN on bearers that do not have a Guaranteed Bit Rate (GBR).

Example

The following command sets the downlink burst rate to use an auto-readjust duration of 2 seconds and lowers the IP precedence of violating packets:

```
apn-ambr rate-limit direction downlink burst-size auto-readjust duration
2 violate-action lower-ip-precedence
```

associate accounting-policy

Associates the APN with specific pre-configured policies configured in the same context.

Product

P-GW

Privilege

Administrator

Syntax

`[ no ] associate accounting-policy` *`name`*

`no`

Removes the selected association from this APN.

`name`

Associates the P-GW APN with an accounting policy configured in the same context. *`name`* must be an existing accounting policy expressed as a string of 1 through 63 characters.
Accounting policies are configured through the **`policy accounting`** command in the Context Configuration mode.

Usage

Use this command to associate the P-GW APN with an accounting policy configured in this context.

Example

The following command associates this P-GW APN with an accounting policy called *`acct1`*:

```
associate accounting-policy acct1
```

authentication

Configures the APN's authentication parameters.

Product

GGSN, P-GW, PDG

Privilege

Security Administrator, Administrator

Syntax

authentication [[**msid-auth** | **imsi-auth** [**password-use-pco** | **username-strip-apn** | **prefer-chap-pco**] | **msisdn-auth** [**password-use-pco** | **username-strip-apn** | **prefer-chap-pco**] | **eap initial-access-request** [**authenticate-authorize** | **authenticate-only**] | [**allow-noauth**] [**chap** *preference* [**convert-to-mschap**]] [**mschap** *preference*] [**pap** *preference*]]

default authentication

default

Sets the default authentication type for this APN. By default **allow-noauth** is the type for authentication for an APN.

msid-auth

Obsolete. Use **imsi-auth**.

imsi-auth

Default: Disabled.
Configures the APN to attempt to authenticate the subscriber based on their International Mobile Subscriber Identification (IMSI) number.

msisdn-auth

Default: Disabled.
Configures the APN to attempt to authenticate the subscriber based on their Mobile Station International Integrated Services Digital Network (MSISDN) number as described in the *Usage* section of this command.

username-strip-apn

Default: Disabled.
This keyword if enabled, either with **msisdn-auth** or **imsi-auth** strips the APN name from the user name *msisdn@apn* or *imsi@apn* received from AAA and makes the user name as *msisdn* or *imsi* respectively.

password-use-pco

Default: Disabled.
This keyword, if enabled, uses the password received through Protocol Configuration Options (PCO) from AAA for authentication.

prefer-chap-pco

Default: Disabled.

If this keyword along with msisdn-auth/imsi-auth is enabled, GGSN performs Challenge Handshake Authentication Protocol (CHAP) authentication, if CHAP parameters are received in Protocol Configuration Options (PCO). However, chap username would be constructed as *msisdn@apn* / *imsi@apn* and chap challenge, chap response parameters should be used as it is from CHAP parameters received in the PCO IE. If CHAP parameters are not received in the PCO IE of the CPC Request, GGSN does normal Password Authentication Protocol (PAP) authentication with PAP username as *msisdn@apn* / *imsi@apn* (ignoring any PAP username if received).

---

eap initial-access-request

Default: Enabled
Configures the type of initial access request to be used in Diameter EAP (Extensible Authentication Protocol) request. This feature is applicable to only Diameter-based AAA interface and not applicable to RADIUS or any other type of AAA interface.

---

authenticate-authorize

Default: Enabled
Configures the "authenticate and authorize" type of initial access request to be used in a Diameter EAP request.

---

authenticate-only

Default: Disabled
Configures the "authenticate only" type of initial access request to be used in a Diameter EAP request.

---

allow-noauth

Default: Enabled
Configures the APN to not perform authentication for PDP contexts as described in the *Usage* section.

---

chap *preference*

Default: Disabled
Configures the APN to attempt to use CHAP to authenticate the subscriber as described in the *Usage* section of this command.
A *preference* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. It must be an integer from 1 through 1000. The lower the integer, the higher the preference.

---

convert-to-mschap

Default: Disabled
If enabled, the CHAP parameters received with the length of 49 bytes, the AAAmgr converts it to MSCHAP.

---

mschap *preference*

Default: Disabled
Configures the APN to attempt to use the Microsoft Challenge Handshake Authentication Protocol (MSCHAP) to authenticate the subscriber as described in the *Usage* section of this command.
A *preference* can be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. It must be an integer from 1 through 1000. The lower the integer, the higher the preference.

pap *preference*

Default: Disabled
Configures the APN to attempt to use PAP to authenticate the subscriber as described in the *Usage* section of this command.
A *preference* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. It must be an integer from 1 through 1000. The lower the integer, the higher the preference.

Usage

Use this command to specify how the APN profile should handle PDP context authentication and what protocols to use (if any). The ability to configure this option is provided to accommodate the fact that not every MS will implement the same authentication protocols.
The authentication process varies depending on whether the PDP context is of type IP or PPP. Table given in this section describes these differences.
For IP PDP contexts, the authentication protocol and values will be passed from the SGSN as Protocol Configuration Options (PCOs) within the create PDP context PDU to the GGSN. The GGSN requires that the authentication protocol is specified by this command (with no regard to priority) and will use this information to authenticate the subscriber.

Table 6. Authentication Process Variances Between PDP Context Type

Authentication Mechanism	IP PDP Context Behavior	PPP PDP Context Behavior
allow-noauth	Allows the session even if the PCOs do not match any of the configured algorithms. If the there was no match and the **aaa constructed-nai authentication** parameter is enabled in the authentication context, the system attempts to determine a subscriber profile (via PAP with no password) using the subscriber's MSISDN as the username.	Allows the session with no authentication algorithm selected. If the **aaa constructed-nai authentication** parameter is enabled in the authentication context, the system attempts to determine a subscriber profile (via PAP with no password) using the subscriber's MSISDN as the username.
chap	If also specified in the PCOs, this protocol will be used to authenticate the subscriber.	Attempts this protocol according to its configured priority. If accepted by the remote end of the PPP connection, this protocol will be used to provide authentication.
mschap	If also specified in the PCOs, this protocol will be used to authenticate the subscriber.	Attempts this protocol according to its configured priority. If accepted by the remote end of the PPP connection, this protocol will be used to provide authentication.
pap	If also specified in the PCOs, this protocol will be used to authenticate the subscriber. If this protocol is used is specified and the **allow-noauth** parameter is disabled, the system will attempt to use the APN's default username/password specified by the **outbound** command for authentication via PAP.	Attempts this protocol according to its configured priority. If accepted by the remote end of the PPP connection, this protocol will be used to provide authentication.
msid-auth	Obsolete. Use **imsi-auth**.	Obsolete. Use **imsi-auth**.

Authentication Mechanism	IP PDP Context Behavior	PPP PDP Context Behavior
imsi-auth	Values in the PCOs are ignored. The subscriber's IMSI is used as the username for PAP authentication. No password is used.	The subscriber's IMSI is used as the username for PAP authentication. No password is used.
msisdn-auth	Values in the PCOs are ignored. The subscriber's MSISDN is used as the username for PAP authentication. No password is used.	Option not available.

Example

The following command would configure the system to attempt subscriber authentication first using MSCHAP, then CHAP, and finally PAP. Since the **allow-noauth** command was also issued, if all attempts to authenticate the subscriber using these protocols fail, then the subscriber would be still be allowed access.

```
authentication mschap 1 chap 2 pap 3 allow-noauth
```

To enable **imsi-auth** or **msisdn-auth**, the following command instances must be issued:

```
authentication imsi-auth
```

```
authentication msisdn-auth
```

bearer-control-mode

Enables or disables the bearer control mode for network controlled QoS (NCQoS) through this APN. It also controls the sending of an IE in GTP messages.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
bearer-control-mode [ mixed | ms-only | none [ prefer-local-value ] ]

default bearer-control-mode
```

default

Sets the bearer control mode to default mode of "none".

mixed

Default: Disabled.
This keyword indicates that the bearer will be controlled by User Equipment (UE) and network side (from GGSN) as well.
To enable network controlled QoS this option must be enabled.

ms-only

Default: Disabled.
This keyword indicates that the bearer will be controlled by the UE side.

none

Default: Enabled.
This keyword indicates that the system will not send any BCM mode information, BCM IE and BCM information in the protocol configuration option (PCO) IE within GTPC messages sent by the GGSN. This option is useful in networks where AGWs or firewalls do not support unknown optional IEs in GTP messages.

prefer-local-value

Default: Disabled.
This keyword indicates that the APN configured with "none" option for bearer control mode will not be overridden by any other interface (e.g. Gx interface towards PCRF). As a result it is ensured that BCM IE is never sent in GTP message.

Important: When bearer control mode is set to "none" with the keyword set "prefer-local-value", even PCRF provided values will not override APN config and therefore sending of BCM mode IE and BCM in PCO IE in CPC Response is supressed.

Usage

Use this command to enable the QoS through bearer control. This can be done either through the MS side or from both the GGSN and MS. To enable network requested QoS user need to enable “Mixed” mode for bearer control.
With this keyword the operator can control sending of BCM information in GTPC messages from the GGSN. With MS-Only or Mixed options in this mode, the system sends the BCM information element in every Create PDP Context Response and Unknown PDP Context Request and Response message.
In some networks AGWs/Firewall drop/reject GTPC messages if there is an Unknown optional IE. To resolve this, the operator can use the “none” option to control sending of BCM IE and BCM information in the PCO IE within GTPC messages from the GGSN.

Example

The following command enables the bearer control from network and MS side for NCQoS.

```
bearer-control-mode mixed
```

cc-home

Configures the home subscriber charging characteristics (CC) used by the GGSN when those from the SGSN will not be accepted.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
cc-home { behavior bits | profile index }

default cc-home
```

default

Restores the cc-home parameter to its default setting of the following:

- **behavior bits:** 0x00
- **profile index:** 8

behavior *bits*

Specifies the behavior bit for the home subscriber charging characteristic. *bits* can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

profile *index*

Specifies the profile index for the home subscriber charging characteristic. *index* can be configured to any integer value between 0 and 15. Default: 8

Important: 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

Usage

When the GGSN is configured to reject the charging characteristics sent by the SGSN for "home" subscribers, it uses the profile index specified by this command to determine the appropriate CCs to use. Multiple behavior bits can be configured for a single profile index by ORing the bit strings together and converting the result to hexadecimal.

The properties of the actual CC profile index are configured as part of the GGSN service using the **cc profile** command. Refer to the *GGSN Service Configuration Mode* chapter of this reference for additional information on this command.

Example

The following command configures a behavior bit of 2 (0000 0000 0010) and a profile index of *10* for home subscribers charging characteristics:

```
cc-home behavior 2 profile 10
```

The following command configures the behavior bits *3* (0000 0000 0100) and 5 (0000 0001 0000 bin) and a profile index of *14* for home subscriber charging characteristics:

```
cc-home behavior 14 profile 14
```

cc-roaming

Configures the roaming subscriber charging characteristics (CC) used by the GGSN when those from the SGSN will not be accepted.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

cc-roaming { **behavior** *bits* | **profile** *index* }

default cc-roaming

default

Restores the cc-roaming parameter to its default setting of the following:

- **behavior bits:** 0x00
- **profile index:** 8

behavior *bits*

Specifies the behavior bit for the roaming subscriber charging characteristic. *bits* can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

profile *index*

Specifies the profile index for the roaming subscriber charging characteristic. *index* can be configured to any integer value between 0 and 15. Default: 8

Important: 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

Usage

When the GGSN is configured to reject the charging characteristics sent by the SGSN for "roaming" subscribers, it uses the profile index specified by this command to determine the appropriate CCs to use. Multiple behavior bits can be configured for a single profile index by ORing the bit strings together and convert the result to hexadecimal.

The properties of the actual CC profile index are configured as part of the GGSN service using the cc profile command. Refer to the GGSN Service Configuration Mode chapter of this reference for additional information on this command.

Example

The following command configures a behavior bit 10 (0010 0000 0000) and a profile index of *10* for roaming subscriber charging characteristics:

```
cc-roaming behavior 200 profile 10
```

The following command configures the behavior bits 9 (0001 0000 0000) and 6 (0000 0010 0000) and a profile index of *14* for roaming subscriber charging characteristics:

```
cc-roaming behavior 120 profile 14
```

cc-sgsn

Specifies the GGSN's source for charging characteristics (CC) - those configured locally or those received from the SGSN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
cc-sgsn { home-subscriber-use-GGSN | radius-returned | roaming-subscriber-use-GGSN |
visiting-subscriber-use-GGSN } +

cc-sgsn { use-GGSN behavior bits profile index[ 0...15 ] [ radius-returned ] }

default cc-sgsn

no cc-sgsn { { radius-returned | home-subscriber-use-GGSN | roaming-subscriber-use-GGSN |
visiting-subscriber-use-GGSN } + | [ use-GGSN ] [ radius-returned ] }
```

default cc-sgsn

Restores the cc-sgsn parameter to its default setting of the following:

- **home-subscriber-use-GGSN**: Disabled
- **roaming-subscriber-use-GGSN**: Disabled
- **visiting-subscriber-use-GGSN**: Disabled

no cc-sgsn

Causes the GGSN to accept CCs from the SGSN(s) when the **no cc-sgsn** command is entered with all applicable keywords. Otherwise, **no cc-sgsn** can be used to turn off one or more of the GGSN sources of CC.

- **roaming-subscriber-use-GGSN**
- **home-subscriber-use-GGSN**
- **roaming-subscriber-use-GGSN**
- **visiting-subscriber-use-GGSN**

Before entering **no cc-sgsn**, it is helpful to determine which CC sources have been configured. This can be done with either **show configuration** or **show apn name** in Exec Mode.

home-subscriber-use-GGSN

Configures the GGSN to use the locally defined charging characteristics for home subscribers, as configured with the APN Configuration Mode **cc-home** command.

radius-returned

Configures the GGSN to accept charging characteristics returned from the RADIUS server for all subscribers for the APN.

roaming-subscriber-use-GGSN

Configures the GGSN to use the locally defined charging characteristics for roaming subscribers, as configured with the APN Configuration Mode **cc-roaming** command.

visiting-subscriber-use-GGSN

Configures the GGSN to use the locally defined charging characteristics for visiting subscribers, as configured with the APN Configuration Mode **cc-visiting** command.

use-GGSN [behavior *bits* **] profile** *index[0...15]*

Configures the GGSN to accept charging characteristics for all subscribers in the APN.
bits specifies the behavior bit for the charging characteristic. This variable can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.
index indicates which profile defined with **cc profile** in GGSN Service Configuration mode, the GGSN will use as a source for CCs. The index can be configured to an integer from 0 to 15.
The **use-GGSN** keyword can be entered alone or in conjunction with the **radius-returned** keyword. When entered, this keyword overrides the previous configuration using any of the home, roaming, and/or visiting keywords.

+

More than one of the above keywords can be entered within a single command.

Usage

This command specifies whether or not CCs received from the SGSN will be accepted. If they are not accepted, the GGSN will use those that have been configured locally.
The GGSN's behavior can be configured for the following subscriber types:

- **Home:** Subscribers belonging to the same Public Land Mobile Network (PLMN) as the one on which the GGSN is located.
- **Roaming:** Subscribers that are serviced by a an SGSN belonging to a different PLMN than the one on which the GGSN is located.
- **Visiting:** Subscribers belonging to a different PLMN than the one on which the GGSN is located.
- Any subscriber in the APN.

Example

The following command instructs the GGSN to accept CCs for any subscriber in the APN based on local profile configurations of CCs.

```
cc-sgsn use-GGSN profile x
```

Assuming the CC source as defined with the previous command, the following command instructs the GGSN to accept CCs supplied by the SGSN(s) and disables the acceptance of CCs supplied by the GGSN for any subscriber within the APN:

```
no cc-sgsn use-GGSN
```

The following command instructs the GGSN to accept CCs for any subscriber in the APN based on CC information returned from the RADIUS server. This command can be issued after the previous command to expand the possible sources.

```
cc-sgsn radius-returned
```

The following command disables the acceptance of CCs supplied by the GGSN for visiting and roaming subscribers:

```
no cc-sgsn roaming-subscriber-use-GGSN visiting-subscriber-use-GGSN
```

cc-visiting

Configures the visiting subscriber charging characteristics (CC) used by the GGSN when those from the SGSN will not be accepted.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

cc-visiting behavior *bits* **profile** *index*

default cc-visiting

default

Restores the cc-visiting parameter to its default setting of the following:

- **behavior bits:** 0x00
- **profile index:** 8

behavior *bits*

Specifies the behavior bit for the visiting subscriber charging characteristic. *bits* can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

profile *index*

Specifies the profile index for the visiting subscriber charging characteristic. *index* can be configured to any integer value between 0 and 15. Default: 8

Important: 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

Usage

When the GGSN is configured to reject the charging characteristics sent by the SGSN for "visiting" subscribers, it uses the profile index specified by this command to determine the appropriate CCs to use. Multiple behavior bits can be configured for a single profile index by ORing the bit strings together and convert the result to hexadecimal.

The properties of the actual CC profile index are configured as part of the GGSN service using the cc profile command. Refer to the GGSN Service Configuration Mode chapter of this reference for additional information on this command.

Example

The following command configures a behavior bit 7 (0000 0100 0000) and a profile index of 10 for visiting subscriber charging characteristics:

```
cc-visiting behavior 40 profile 10
```

The following command configures the behavior bits 1 (0000 0000 0001) and 12 (1000 0000 0000) and a profile index of 14 for visiting subscriber charging characteristics:

```
cc-visiting behavior 801 profile 14
```

content-filtering category

Enables or disables the specified pre-configured Category Policy Identifier for Category-based Content Filtering support.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

content-filtering category policy-id*cf_policy_id*

no content-filtering category policy-id

no

Disables the previously configured category policy identifier for Content Filtering support to the APN. This is the default setting.

policy-id *cf_policy_id*

Applies the specified content filtering category policy ID, configured in the ACS Configuration Mode, to this APN.
cf_policy_id must be a category policy ID entered as an integer from 1 through 4294967295.
If the specified category policy ID is not configured in the ACS Configuration Mode, all packets will be passed regardless of the categories determined for such packets.

Important: Category Policy ID configured through this mode overrides the Category Policy ID configured through **content-filtering category policy-id** command in the ACS Rulebase Configuration Mode.

Usage

Use this command to enter the Content Filtering Policy Configuration Mode and to enable or disable the Content Filtering Category Policy ID for an APN.

Important: If Content Filtering Category Policy ID is not specified here the similar command in the ACS Rulebase Configuration Mode determines the policy.

Up to 64 different policy IDs can be defined.

Example

The following command enters the Content Filtering Policy Configuration Mode and enables the Category Policy ID *101* for Content Filtering support:

```
content-filtering category policy-id 101
```

credit-control-group

Configures the credit control group to be used for subscribers who use this APN.

Product

GGSN, ECS, P-GW

Privilege

Security Administrator, Administrator

Syntax

credit-control-group *cc_group_name*

no credit-control-group

no

Removes the previously configured credit control group from the APN configuration.

cc_group_name

Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the credit control group for this APN.
Creating different credit control groups enables applying different credit control configurations (DCCA dictionary, failure-handling, session-failover, Diameter endpoint selection, etc.) to different subscribers on the same system.
Without credit control groups, only one credit control configuration is possible on a system. All the subscribers in the system will have to use the same configuration.

Example

The following command configures a credit control group named *testgroup12* for the current APN:

```
credit-control-group testgroup12
```

data-tunnel mtu

Configures the Maximum Transmission Unit (MTU) for data sent on the IPv6 tunnel between the P-GW and the mobile node.

Product

P-GW

Privilege

Administrator

Syntax

data-tunnel mtu*bytes*

default data-tunnel mtu

default

Returns the command to the default value of 1500.

bytes

Specifies the MTU for the IPv6 tunnel between the P-GW and the mobile node. *bytes* must be an integer between 1280 and 2000. Default: 1500

Usage

Use this command to set the MTU for data traffic on the IPv6 tunnel between the P-GW and the mobile node.

Example

The following command sets the MTU for IPv6 data traffic to *1400* bytes:

```
data-tunnel mtu 1400
```

data-tunneling ignore df-bit

Controls the handling of the DF (Don't Fragment) bit present in the user IPv4/IPv6 packet for tunneling used for the Mobile IP data path.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] data-tunneling ignore df-bit
```

default

Restores the data-tunneling parameter to its default setting of disabled.

no

Disables this option. The DF bit in the tunneled IP packet header is not ignored during tunneling. This is the default setting.

ignore df-bit

Ignores the DF bit in the tunneled IP packet header during tunneling. This is the default setting.

Usage

Use this command to configure a user so that during Mobile IP tunneling the DF bit is ignored and packets are fragmented.
If this feature is enabled, and fragmentation is required for the tunneled user IPv4/IPv6 packet, then the DF bit is ignored and the packet is fragmented. Also the DF bit is not copied to the outer header.
In the GGSN, this command also affects the other L3 tunneling options, IP-in-IP and GRE, but does not affect L2TP tunneling.

Example

To enable fragmentation of a subscribers packets over a MIP tunnel even when the DF bit is present, enter the following command:

```
data-tunneling ignore df-bit
```

dcca origin endpoint

This command is obsolete. To configure the Diameter Credit Control Origin Endpoint, in the Credit Control Configuration Mode, use the **diameter origin endpoint** command.

dcca peer-select

Specifies the Diameter credit control primary and secondary host for credit control.

Product

GGSN, ECS, P-GW

Privilege

Security Administrator, Administrator

Syntax

dcca peer-select peer *host_name* [**realm** *realm_name*] [**secondary-peer** *host_name*]

no dcca peer-select

no

Removes the previously configured Diameter credit control peer selection.

host_name

Specifies a unique name for the peer as an alphanumeric string of 1 through 63 characters that allows punctuation marks.

realm *realm_name*

Specifies the ream as an alphanumeric string of from 1 through 127 characters that allows punctuation marks. The realm may typically be a company or service name.

secondary-peer *host_name*

Specifies a back-up host that is used for fail-over processing as an alphanumeric string of from 1 through 63 characters. When the route-table does not find an AVAILABLE route, the secondary host performs fail-over processing.

Usage

Use this command to select a Diameter credit control peer and realm.

WARNING: This configuration completely overrides all instances of **diameter peer-select** that have been configured within the Credit Control Configuration Mode for an Active Charging Service.

Example

The following command selects a Diameter credit control peer named test and a realm of *companyx*:

```
dcca peer-select test realm companyx
```

dhcp context-name

Configures the name of the context on the system in which Dynamic Host Control Protocol (DHCP) functionality is configured.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] dhcp context-name name
```

no

Removes a previously configured context name.

name

Specifies the name of a context configured on the system in which one or more DHCP services are configured. *name* is an alphanumeric string of 1 through 79 characters that is case sensitive.

Usage

If the APN is to support dynamic address assignment via DHCP (either the proxy or relay mode), this parameter must be configured to point the APN to the name of a pre-configured context on the chassis in which one or more DHCP services are configured.
The command can be used to identify a single DHCP service instance within the specified context to use to facilitate the address assignment.

Example

The following command configures the APN to look for DHCP services in a context called *dhcp-ctx:*

```
dhcp context-name dhcp-ctx
```

dhcp lease-expiration-policy

Configures the system's handling of PDP contexts whose DHCP assigned IP lease has expired.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
dhcp lease-expiration-policy { auto-renew | disconnect }

default dhcp lease-expiration-policy
```

default

Restores the dhcp lease-expiration-policy parameter to its default setting of auto-renew.

auto-renew

Configures the system to automatically renew an IP address' lease when it is about to expire for PDP contexts facilitated by the APN. Default: Enabled

disconnect

Configures the system to automatically release the PDP context when the lease for the IP address associated with that context expires. Default: Disabled

Usage

Use this command to specify the action the system is to take when leases for IP addresses for PDP contexts that it are currently facilitated by the current APN are about to expire.

Example

The following command causes the system to release PDP contexts associated with the current APN when the lease for their DHCP-assigned IP address expires:

```
dhcp lease-expiration-policy disconnect
```

dhcp service-name

Configures the name of a specific DHCP service to use when dynamically assigning IP addresses to PDP contexts using the Dynamic Host Control Protocol.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] dhcp service-name svc_name
```

no

Removes a previously configured DHCP service name.

svc_name

Configures the name of the DHCP service instance that is to be used by the current APN for the dynamic assignment of IP addresses to PDP contexts. The name can be an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage

Use this command to specify a pre-configured DHCP service instance that is to be used by the APN for IP address assignment when the Dynamic Host Control Protocol is used.
The name of the context in which the desired DHCP service is configured must be specified by the **dhcp context-name** command.

Example

The following command instructs the APN to use a DHCP service called *dhcp1*:

```
dhcp service-name dhcp1
```

dns

Configures the Domain Name Service (DNS) servers that will be used by the APN for PPP.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

dns { **primary** | **secondary** } { *address* }

no dns { **primary** | **secondary** } [*dns_address*]

no

Deletes a previously configured DNS server.

primary

Configures the primary DNS server for the APN.

secondary

Configures the secondary DNS server for the APN. Only one secondary DNS server can be configured.

address

Configures the IP address of the DNS server expressed in IPv4 dotted-decimal notation.
Default: primary = 0.0.0.0, secondary = 0.0.0.0

dns_address

Specifies the IP address of the DNS server to remove, expressed in IPv4 dotted-decimal notation.

Usage

DNS servers are configured on a per-APN profile basis. This allows each APN profile to use specific servers in processing PDP contexts.
The configured DNS IP addresses are relayed to the subscriber within IPCP if the PDP type is PPP, or as PCOs (Protocol Configuration Options) if the PDP type is IP.
The DNS can be specified at the APN level in APN configuration as well as at the Context level in Context configuration mode with **ip name-servers** command, or it can be received from AAA server.
When DNS is requested in PCO configuration, the following preference will be followed for DNS value:
1. DNS Values received from LNS have the first preference.
2. DNS values received from RADIUS Server has the second preference.
3. DNS values locally configured with APN has the third preference.
4. DNS values configured at context level with **ip name-servers** command has the last preference.

Important: The same preference would be applicable for the NBNS (NetBIOS Name Service) servers to be negotiated via ICPC (Initial Connection Protocol Control) with the LNS (L2TP Network Server).

Example

The following commands configure a primary DNS server address of *192.168.100.3* and a secondary DNS server address of *192.168.100.4*:

```
dns primary 192.168.100.3

dns secondary 192.168.100.4
```

ehrpd-access

Configures the P-GW to exclude IPv6 traffic from being delivered to UEs, accessing PDNs from the eHRPD network that do not have IPv6 capabilities.

Product

P-GW

Privilege

Administrator

Syntax

[default | no] ehrpd-access drop-ipv6-traffic

[default | no]

Resets this command to its default setting of disabled.

drop-ipv6-traffic

Excludes IPv6 traffic from being delivered to UEs, accessing PDNs from the eHRPD network that do not have IPv6 capabilities.

Usage

Use this command to exclude IPv6 traffic from being delivered to UEs on the eHRPD network that do not have IPv6 capabilities.

emergency-apn

Configures this APN as an emergency APN for Voice over LTE (VoLTE) based E911 support.

Product

P-GW

Privilege

Administrator

Syntax

```
[ default | no ] emergency-apn
```

[default | no]

Resets this command to its default setting of disabled.

Usage

Use this command to configure this APN as an emergency APN for VoLTE based E911 support. With this support, a UE is able to connect to an emergency PDN and make Enhanced 911 (E911) calls while providing the required location information to the Public Safety Access Point (PSAP).
E911 is a telecommunications-based system that is designed to link people who are experiencing an emergency with the public resources that can help. This feature supports E911-based calls across the LTE and IMS networks. In a voice over LTE scenario, the subscriber attaches to a dedicated packet data network (PDN) called EPDN (Emergency PDN) in order to establish a voice over IP connection to the PSAP. Both signaling and RTP media flow over a dedicated emergency bearer. Additionally, different than normal PDN attachment that relies on AAA and PCRF components for call establishment, the EPDN attributes are configured locally on the P-GW, which eliminates the potential for emergency call failure if either of these systems is not available.

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

firewall policy

Eenables or disables Stateful Firewall support for the APN.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
firewall policy firewall-required

[ default | no ] firewall policy
```

no

Disables Stateful Firewall support for this APN.

default

Configures the default setting for Stateful Firewall support.
Default: Disabled

Usage

Use this command to enable or disable Stateful Firewall support for this APN.

Important: This command is only available in StarOS 8.0. In StarOS 8.1 and later, this configuration is available in the ACS Rulebase Configuration Mode.

Important: Unless Stateful Firewall support for this APN is enabled using this command, firewall processing for this APN is disabled.

Important: If firewall is enabled, and the rulebase has no firewall configuration, Stateful Firewall will cause all packets to be discarded.

Example

The following command enables Stateful Firewall support for an APN:

```
firewall policy firewall-required
```

The following command disables Stateful Firewall support for an APN:

```
no firewall policy
```

fw-and-nat policy

Configures the Firewall-and-NAT policy to be used for subscribers who use this APN.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

fw-and-nat policy *fw_nat_policy*

[default | no] fw-and-nat policy

default

Configures the default setting.
Default: The default Firewall-and-NAT policy configured in the rulebase is used for subscribers who use this APN.

no

Disables Firewall and NAT for the APN.

fw_nat_policy

Specifies the Firewall-and-NAT policy for the APN as an alphanumeric string of 1 through 63 characters. Note that this policy will override the **default Firewall-and-NAT policy** configured in the ACS rulebase.

Usage

Use this command to configure the Firewall-and-NAT policy for the APN. Note that the policy configured in the subscriber mode will override the default policy configured in the ACS rulebase. If a policy is not configured in the subscriber mode, the default policy configured in the ACS rulebase will be used.

Important: This command is customer-specific and is only available in StarOS 8.1.

Important: This customer-specific command must be used to configure the Policy-based Firewall-and-NAT feature.

Example

The following command configures a Firewall-and-NAT policy named *standard* for the APN:

```
fw-and-nat policy standard
```

gsm-qos negotiate

Enables negotiation of the QoS Reliability Class attribute based on the configuration provided for Service Data Unit (SDU) Error Ratio and Residual Bit Error Ratio (BER) attributes in the APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

gsm-qos negotiate sdu-error-ratio *sdu-error-ratio-code* [**residual-ber** *residual-ber-code*]

[**no**] **gsm-qos negotiate sdu-error-ratio** [*sdu-error-ratio-code* [**residual-ber** *residual-ber-code*]]

no

Disables negotiation of the QoS Reliability Class attribute.

sdu-error-ratio *sdu-error-ratio-code*

Enables the negotiation of the QoS Reliability Class attribute based on Service Data Unit (SDU) Error Ratio attributes. *sdu-error-ratio-code* corresponds to distinct SDU Error ratio values within an integer range of 1 to 7.

residual-ber *residual-ber-code*

Enables the optional configuration of negotiation of the QoS Reliability Class attribute based on Residual Bit Error Ratio (BER) attributes. *residual-ber-code* corresponds to distinct Residual Bit Error Ratio values within an integer range of 1 to 9.

Usage

This command configures the QoS attribute Reliability Class to be negotiated based on the configuration provided for SDU Error Ratio and Residual BER attributes. The derived Reliability Class and the configured values for SDU Error Ratio and Residual BER are sent back in CPC and UPC response.
The mapping for *sdu-error-ratio-code* is as follows:

Code	Value
1	10-2
2	7*10-3
3	10-3
4	10-4
5	10-5
6	10-6
7	10-1

Residual BER needs to be specified when SDU Error Ratio is set to codes 1, 2, 3 or 7 (Or, SDU Error Ratio is intended to be set to a value greater than 5*10-4), for determining the Reliability Class QoS attribute. Otherwise, the Residual BER value received in the Create PDP context request QoS (or UPC request) would be used. The mapping for *residual-ber-code* is as follows:

Code	Value
1	5*10-2
2	10-2
3	5*10-3
4	4*10-3
5	10-3
6	10-4
7	10-5
8	10-6
9	6*10-8

Example

The following commands configures the negotiation of QoS attribute Reliability Class based on Service Data Unit (SDU) Error Ratio *3* attributes in the APN:

```
gsm-qos negotiate sdu-error-ratio 3
```

gtpp group

Enables a configured GTPP server group to an APN for CGF accounting functionality.

Important: In Releases prior to 11.0, only one GTPP group is allowed to configure per APN. In Releases 11.0 and later, this CLI can be used to configure up to a maximum of 32 GTPP groups for each APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

gtpp group *group_name* [**accounting-context** *ac_context_name*]

default gtpp group

no gtpp group *group_name*

no

Removes all the configured GTPP groups for the specific APN.

group_name

Specifies the name of server group that is used for authentication/accounting for specific APN. *group_name* must be an alphanumeric string of 1 to 63 characters. It must be identical to the one configured earlier within the same APN context.

Important: In Release 11.0 and later, if you have mistakenly configured a GTPP group, you should remove the initially configured group and configure the new desired group. However, in Releases prior to 11.0, there is no need to remove the incorrect configuration; instead you can directly reconfigure the desired GTPP group.

Important: If a GTPP group entry is invalid, this GTPP group will be ignored and the next valid GTPP group in the APN will be used. If no valid GTTP group exists, then the default GTPP group in the accounting context specified by the GGSN service will be used.

accounting-context *ac_context_name*

Specifies the name of an accounting context on the system that processes accounting for PDP contexts handled by this GGSN service for accounting to specific APN.
ac_context_name must be an alphanumeric string of 1 through 79 characters that is case sensitive.
Note that if an accounting context is not specified here, the system uses the GGSN service context or the context configured by the **accounting context** command in the GGSN Service Configuration mode.

Usage

This feature provides the GTPP server configurables under a GTPP group node. Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual an GTPP server group for subscribers in that context. Each server group consists of a list of CGF (Charging Group Function) accounting servers.
In case no GTPP group is applied for the said APN or default APN template, then the default GTPP server group available at the context level is applicable for accounting of a specific APN.

Important: When multiple GTPP groups are applied to the same APN, the load will be shared across these GTPP groups. Sessions for this APN will use all the configured GTPP groups in a round robin fashion.

Once a GTPP group is selected for a subscriber session, the GTPP group will never change under any circumstances. A request is initially sent to primary CGF server configured in that group. When the primary fails to respond, the request is sent to secondary CGF server.
The process of failover from primary to secondary is per the 3GPP standards. Multiple GTPP groups configuration is actually supported only for load sharing of sessions within an APN and not used for failover. When all CGFs are down in a GTPP group, the requests are archived either in hard disk or main memory depending on whether or not streaming is enabled.

Example

The following command applies a previously configured GTPP server group named *star1* to an APN within the specific context:

```
gtpp group star1
```

The following command disables the applied GTPP server group for the specific APN:

```
no gtpp group star1
```

gtpp secondary-group

Enables or associates a preconfigured secondary GTPP server group to an APN for CGF (Charging Group Function) accounting functionality. By default it is disabled.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

gtpp secondary-group *group_name* [**accounting-context** *actt_ctxt_name*]

[**default** | **no**] **gtpp secondary-group** *group_name*

default

Default: Enabled
Restores the default mode for secondary GTPP group for APN template.

no

Disables the configured/associated GTPP secondary group for specific APN.

group_name

Specifies the name of secondary GTPP server group that is used as an alternate for the primary GTPP group associated with a specific APN for storage of GTPP messages. *group_name* must be an alphanumeric string of 1 through 63 characters. It must be the same name as configured earlier within the same APN context.

accounting-context *actt_ctxt_name*

Specifies the name of an accounting context on the system that processes accounting for PDP contexts handled by this GGSN service for accounting to a specific APN.
actt_ctxt_name specifies the name of the context to be used for accounting as an alphanumeric string of 1 through 79 characters that is case sensitive.
Note that if an accounting context is not specified here, the system uses the GGSN service context or the context configured by the **accounting context** command in the GGSN Service Configuration mode.

Usage

Use this feature to provide the secondary GTPP server group support for an APN.
When the secondary GTPP group is configured with this command, the GTPP messages will also be mirrored to the secondary servers.
This secondary group configuration is ignored, if the configured *group_name* is the same as the primary group. It will also be ignored, if the configured GTPP *group_name* and/or accounting context *ac_context_name* is invalid. In such cases, the call will be established successfully (unlike the primary group configuration where the call drops).
In the absence of a configured *ac_context_name* context, the GGSN service context is chosen by default.
The secondary group messages are low priority and thus are purged when there is no room for the new messages.
For more information on GTPP group, refer the description of the **gtpp group** command.

Example

The following command applies a previously configured GTPP server group named *star2* to as secondary GTPP group to an APN within the specific context:

```
gtpp secondary-group star2
```

The following command disables the applied secondary GTPP server group for the specific APN:

```
no gtpp secondary-group star2
```

idle-timeout-activity

Configures a session idle-timeout to be reset with uplink packets only, or with both uplink and downlink packets.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] idle-timeout-activity ignore-downlink

default idle-timeout-activity
```

default

Sets or restores the command to the default setting.

ignore-downlink

Sets the system to ignore the downlink traffic for consideration as activity for idle-timeout.

Usage

If **idle-timeout-activity ignore-downlink** is configured, the downlink (network to subscriber) traffic will not be used to reset the idle-timeout. Only uplink (subscriber to network) packets will be able to reset the idle-timeout.
By default, **ignore-downlink** is negated by the **no** command so downlink traffic is also used to reset the idle-timeout.

Example

The following command causes both uplink and downlink traffic to reset a session idle-timeout:

```
default idle-timeout-activity
```

The following command causes the session idle-timeout to be reset with only uplink packets:

```
idle-timeout-activity ignore-downlink
```

ims-auth-service

Applies an IMS (IP Multimedia Subsystem) authorization service to a subscriber through APN for Gx interface support and functionality.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ims-auth-service auth_svc_name
```

no

Disables the applied IMS authorization service for a specific APN.

auth_svc_name

Specifies the name of the IMS authorization service name that is used for Gx interface authentication for a specific APN. *auth_svc_name* must be a alphanumeric string of 1 through 63 characters preconfigured within the same context as this APN.

Usage

This feature provides the IMS authorization service configuration for Gx interface in IMS service node.

Example

The following command applies a previously configured IMS authorization service named *gx_interface1* to an APN within the specific context:

```
ims-auth-service gx_interface1
```

The following command disables the applied IMS authorization service *gx_interface1* for the specific APN:

```
no ims-auth-service gx_interface1
```

ip access-group

Configures an IPv4/IPv6 access group for the current APN profile.

Product

GGSN, ECS, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ip access-group acl_group_name [ in | out ]
```

no

Removes a previously configured IPv4/IPv6 access group association.

acl_group_name

Specifies the name of the IPv4/IPv6 access group. *acl_group_name* is a previously configured ACL group expressed as an alphanumeric string of 1 to 79 characters.

in | out

Default: both (in and out)
Specifies the access-group as either inbound or outbound by the keywords **in** and **out**, respectively.

Usage

Use this command to apply a single IPv4/IPv6 access control list to multiple subscribers via this APN for inbound or outbound IPv4/IPv6 traffic.
If no traffic direction is specified, the selected access control list will be applied to both directions.

Example

The following command associates the *sampleipv4Group* access group with the current APN profile for both inbound and outbound access.

```
ip access-group sampleipv4Group
```

The following command removes the outbound access group flag for *sampleipv4Group*.

```
no ip access-group sampleipv4Group out
```

ip address alloc-method

Configures the method by which this APN will obtain IP addresses for PDP contexts.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
ip address alloc-method { dhcp-proxy [ allow-deferred ] [ prefer-dhcp-options ] | dhcp-relay | local [ allow-deferred ] | no-dynamic [ allow-deferred ] } [ allow-user-specified ]

default ip address allocation-method
```

default

Restores the APN ip parameters to the following default settings.

dhcp-proxy

Default: Disabled
Configures the APN to assign an IP address received from a DHCP server.

Important: If this option is used, the system's DHCP parameters must be configured.

dhcp-relay

Configures the APN to forward DHCP packets received from the MS to a DHCP server. Default: Disabled

Important: If this option is used, the system's DHCP parameters must be configured.

local

Configures the APN to allocate IP addresses from a pool configured in the destination context on the system. Default: Enabled

Important: If this option is used, the name of the IP address pool from which to allocate addresses must be configured using the **ip address pool-name** command. If no pool name is specified, the system will attempt to allocate an address from any public pool configured in the destination context.

no-dynamic

Disables the dynamic assignment of IP addresses to PDP contexts using this APN. Default: Disabled
If a PDP context needing an IP address is received by an APN with this option enabled, it will be rejected with a cause code of 220 (Unknown PDP address or PDP type).

prefer-dhcp-options

If this keyword is specified with **dhcp-proxy** for IP address allocation configuration, the GGSN will prefer DHCP-supplied parameters over values provided by AAA server or by local configuration. This keyword controls the following parameters:

- primary and secondary Domain Name Server (DNS) addresses
- primary and secondary NetBIOS Name Server (NBNS) addresses

These values will be sent out in the PCO IE of a GTP Create PDP Response Message whenever the MS Requests them in A Create PDP Request Message.
Default: Disabled

Important: This keyword is available only with dhcp-proxy ip allocation method as this functionality is implemented only for GGSN acting as DHCP proxy.

By default, this functionality is disabled. Hence, DNS and NBNS values received from a DHCP server will not be considered by the GGSN.

allow-deferred

Enables support for P-GW deferred address allocation. Default: Disabled

allow-user-specified

Enables support for PDP contexts requesting the use of specific (static) addresses. Default: Enabled

Important: If this option is not enabled, PDP contexts requesting the use of a static address will be rejected with a cause code of 220 (Unknown PDP address or PDP type).

Usage

Use this command to configure the method by which the APN profile will assign IP addresses to PDP contexts.
When the PDP context is being established and the APN name is determined, the system will examine the APN's configuration profile. Part of that procedure is determining how to handle IP address allocation. The figure in the Example section below displays the process used by the system to determine how the address should be allocated.

Example

The following command configures the APN to dynamically assign an address from a DHCP server and reject PDP sessions with static IP addresses:

```
ip address alloc-method dhcp-proxy
```

The following command configures the APN to reject sessions requesting dynamically assigned addresses and only allow those with static addresses:

```
ip address alloc-method no-dynamic allow-user-specified
```

The following figure provides the IP address allocation process:

Figure 3. IP Address Allocation Process

ip address pool

Configures the name of a a private IP address pool configured on the system from which to assign an address for a PDP context.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ip address pool name pool_name
```

no

Removes a previously configured pool name.

pool_name

Specifies the name of the private pool configured on the system from which an IP address will be assigned. The name is expressed as an alphanumeric string of 1 through 31 characters that is case sensitive.

Usage

If the **ip address alloc-method** command is configured to allow the assignment of IP addresses from a local pool configured on the system. It command instructs the system as to which pool should be used.
The pool specified by this command must be a private pool configured in the destination context on the system. Please refer to the **ip pool** command in the *Context Configuration Mode Commands* chapter for information on configuring IP address pools.
Multiple APNs can use the same IP address pool if required. In addition, this command could be issued multiple times to allow a single APN to use different address pools.

Example

The following command configures the system to use a pool named *private_pool1* for address allocation:

```
ip address pool private_pool1
```

ip context-name

Configures the name of the destination context to use for subscribers accessing this APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ip context-name ctxt_name
```

no

Removes a previously configured context name.

ctxt_name

Specifies the name of the context through which subscriber data traffic will be routed. *ctxt_name* must be an alphanumeric string from 1 to 79 characters.

Usage

Use this command to specify the name of a destination context configured on the system through which to route all subscriber data traffic. This context will be used for subscribers accessing this APN. If no name is specified, the system will use the context in which the APN is configured as the destination context.
When the APN is used to support Mobile IP functionality, this command is used to indicate the context in which the FA (foreign Agent) service is configured. If no name is specified, the context in which the GGSN service facilitating the subscriber PDP context is used.

Example

The following command configures the system to route subscriber traffic for the APN through a context called isp1:

```
ip context-name isp1
```

ip header-compression

Configures IP packet header compression parameters for this APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
ip header-compression vj

default ip header-compression

no ip header-compression
```

default

Disables Van-Jacobson header compression.

no

Disables Van-Jacobson header compression.

vj

Enables Van-Jacobson header compression for IP packets. Default: Enabled

Usage

IP header compression reduces packet header overhead resulting in more efficient utilization of available bandwidth.

Example

The following command disables packet header compression for the APN:

```
no ip header-compression
```

ip hide-service-address

Renders the IP address of the GGSN unreachable from mobile stations (MSs) using this APN. This command is configured on a per-APN basis.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] ip hide-service-address
```

default

Does not allow the mobile station to reach the GGSN IP address using this APN.

no

Allows the mobile station to reach the GGSN IP address using this APN.

Usage

This hides the GGSN IP address from the mobile station for security purposes.

Example

The following command allows the GGSN's IP address to be viewed by the mobile station:

```
no ip hide-service-address
```

ip local-address

Configures the local-side IP address of the subscriber's point-to-point connection.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

ip local-address *ip_address*

no ip local-address

no

Removes a previously configured IP local-address.

ip_address

Specifies an IP address configured in a destination context on the system through which a packet data network can be accessed. *ip_address* must be expressed in IPv4 dotted-decimal notation.

Usage

This parameter specifies the IP address on the system that the MS uses as the remote-end of the PPP connection. If no local address is configured, the system uses an unnumbered scheme for local-side addresses.

Example

The following command configures a local address of 192.168.1.23 for the MS:

```
ip local-address 192.168.1.23
```

ip multicast discard

Configures the IP multicast discard packet behavior.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] ip multicast discard
```

default

Restores the APN IP parameters to the default multicast settings, which is to discard PDUs.

no

Removes a previously configured IP multicast discard.

Usage

This command specifies if IP multicast discard is enabled or disabled.

Example

The following command enables IP multicast discard for an APN:

```
ip multicast discard
```

ip qos-dscp

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets of a particular 3GPP QoS class over the Gi interface.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
ip qos-dscp { qci { 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 } { dscp } } +

default ip qos-dscp

no ip qos-dscp { qci { 1 | 2 | 3 | 4 | 5 { allocation-retention-priority { 1..3 } } | 6 {
allocation-retention-priority { 1..3 } } | 7 { allocation-retention-priority { 1..3 } } |
8 { allocation-retention-priority { 1..3 } } | 9 } } } +
```

default

Restores the APN IP parameters to the default setting *conversational ef streaming af11 interactive af21 background be*.

no

Restores the QoS parameter to its default setting.

allocation-retention-priority

Specifies the DSCP for interactive class if the allocation priority is present in the QoS profile.
allocation-retention-priority can be the integers 1, 2, or 3.
DSCP values use the following matrix to map based on traffic handling priority and Alloc/Retention priority if the allocation priority is present in the QoS profile.
Following table shows the DSCP value matrix for *allocation-retention-priority*.

Table 7. Default DSCP Value Matrix

Allocation Priority	1	2	3
Traffic Handling Priority			
1	ef	ef	ef
2	ef	ef	ef
3	af21	af21	af21
4	af21	af21	af21

Important: If you only configure DCSP marking for interactive traffic classes without specifying ARP, it may not properly take effect. The CLI allows this scenario for backward compatibility. However, it is recommended that you configure all three values.

qci

Configures the QoS Class Identifier (QCI) attribute of QoS. Here the *qci_val* is the QCI for which the negotiate limit is being set; it ranges from 1 to 9.

dscp

Specifies the DSCP for the specified traffic pattern. *dscp* can be configured to any one of the following:

• **af11:** Assured Forwarding 11 per-hop-behavior (PHB)	• **af33:** Assured Forwarding 33 PHB
• **af12:** Assured Forwarding 12 PHB	• **af41:** Assured Forwarding 41 PHB
• **af13:** Assured Forwarding 13 PHB	• **af42:** Assured Forwarding 42 PHB
• **af21:** Assured Forwarding 21 PHB	• **af43:** Assured Forwarding 43 PHB
• **af22:** Assured Forwarding 22 PHB	• **be:** Best effort forwarding PHB
• **af23:** Assured Forwarding 23 PHB	• **ef:** Expedited forwarding PHB
• **af31:** Assured Forwarding 31 PHB	• **pt:** Pass through (ToS of user packet is not modified)
• **af32:** Assured Forwarding 32 PHB	

Default: QCI:

- 1: ef
- 2: ef
- 3: af11
- 4: af11
- 5: ef
- 6: ef
- 7: af21
- 8: af21
- 9: be

+

More than one of the above keywords can be entered within a single command.

Usage

DSCP levels can be assigned to specific traffic patterns in order to ensure that data packets are delivered according to the precedence with which they're tagged. The diffserv markings are applied to the IP header of every subscriber data packet transmitted over the Gi interface(s).
The traffic patterns are defined by QCI (1 to 9). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in following tables respectively:

Table 8. Class structure for assured forwarding (af) levels

Drop Precedence	Class			
	Class 1	Class 2	Class 3	Class 4
Low	af11	af21	af31	af41
Medium	af12	af22	af32	af41
High	af13	af23	af33	af43

Precedence (low to high)	DSCP
1	Best Effort (be)
2	Class 1
3	Class 2
4	Class 3
5	Class 4
6	Express Forwarding (ef)

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

Example

The following command configures the DSCP level for QCI to be Expedited Forwarding,**ef**:

```
ip qos-dscp qci 1 ef
```

ip source-violation

Enables or disables packet source validation for the current APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

ip source-violation { **ignore** | **check** [**drop-limit** *limit*] } [**exclude-from-accounting**]

default ip source-violation

default

Restores the APN ip parameters to the default settings **check** *enabled*, **drop-limit** *10*.

ignore

Default: Disabled
Disables source address checking for the APN.

check [drop-limit *limit* **]**

Default: Enabled, limit = 10
Enables the checking of source addresses received from subscribers for violations.
A **drop-limit** can be configured to set a limit on the number of invalid packets that can be received from a subscriber prior to their session being deleted. *limit* can be configured to any integer value between 0 and 1000000. A value of 0 indicates that all invalid packets will be discarded but the session will never be deleted by the system.

exclude-from-accounting

Default: Disabled
Excludes the packets identified with IP source violation from the statistics generated for accounting records.

Usage

Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.
Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

Example

The following command enables source address validation for the APN and configures a drop-limit of *15*:

```
ip source-violation check drop-limit 15
```

ip user-datagram-tos copy

Controls the copying of the IP ToS octet value from user IPv4/IPv6 datagrams into the IP header of GTP tunnel encapsulations.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] ip user-datagram-tos copy
```

default

Sets the default behavior of this command. By default this function is disabled.

no

Removes the preconfigured parameter for this command.

Usage

This command enables or disables the copying of the ToS byte from the inner IP header to the outer IP header for an RP connection.
When this function is enabled, the SGSN can detect the special ToS marking in the outer IP header of GTP tunnel packets and identify certain packets as control messages.

ipv6 access-group

Configures the IPv6 access group for the current APN profile which applies a single Access Control List (ACL) to multiple subscribers via the APN for IPv6 traffic.

Product

GGSN, ECS, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ipv6 access-group group_name [ in | out ]
```

no

Removes a previously configured IPv6 ACL applied to a particular APN for IPv6 traffic. If at least one of the two **{ in | out }** options is not selected for the ACL that will be removed, the ACL will be removed for both directions.

group_name

Specifies the name of the IPv6 access group as an alphanumeric string of 1 through 79 characters.

[in | out]

Default: both (in and out)
Specifies the access-group as either inbound or outbound by the keywords **in** and **out**, respectively.
If no direction is supplied in the base command, the specified IPv6 access control list will be applied to both directions.

Usage

Use this command to apply a single IPv6 access control list to multiple subscribers via an APN for inbound or outbound IPv6 traffic.
If no traffic direction is specified, the selected access control list will be applied to both traffic directions.

Example

The following command associates the *sampleipv6Group* access group with the current APN profile for both inbound and outbound access:

```
ipv6 access-group sampleipv6Group
```

The following removes the outbound access group flag for *sampleipv6Group*:

```
no ipv6 access-group sampleipv6Group out
```

ipv6 dns

Configures primary and secondary IPv6 Domain Name Service (DNS) servers.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ipv6 dns { primary | secondary } { ipv6_dns_address }
```

no

Deletes a previously configured DNS server.

primary

Configures the IPv6 address of primary DNS server for the APN.

secondary

Configures IPv6 address of the secondary DNS server for the APN. Only one secondary DNS server can be configured.

ipv6_dns_address

The IP address of the DNS server entered using IPv6 colon-separated notation.

Usage

DNS servers are configured on a per-APN profile basis. This allows each APN profile to use specific servers in processing PDP contexts.
The DNS can be specified at the APN level in APN configuration as well as at the Context level in Context configuration mode with **ip name-servers** command, or it can be received from AAA server.
When DNS is requested in PCO configuration, the following preference will be followed for DNS value:
1. DNS Values received from LNS have the first preference
2. DNS values received from RADIUS Server has the second preference
3. DNS values locally configured with APN has the third preference
4. DNS values configured at context level with **ip name-servers** command has the last preference.

Important: The same preference would be applicable for the NBNS (NetBIOS Name Service) servers to be negotiated via ICPC (Initial Connection Protocol Control) with the LNS (L2TP Network Server).

Example

The following command provides an example of setting the primary DNS server:

```
ipv6 dns primary fe80::c0a8:a04
```

ipv6 egress-address-filtering

Enables or disable IIPv6 egress address filtering. This function filters out packets not meant for the mobile interface ID. The GGSN records the source interface ID of all the packets received from the mobile node. When packets sent to the mobile node are received, the destination interface ID is compared against the list of recorded interface IDs and with the local interface-ID assigned to the MS during IPv6CP. If no match is found, the packet is dropped.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ipv6 egress-address-filtering
```

no

Disables IPv6 egress address filtering.

Usage

Used to filter packets that arrive from the internet to a particular site.

Example

The following command provides an example disabling egress address filtering:

```
no ipv6 egress-address-filtering
```

ipv6 initial-router-advt

Creates an IPv6 initial router advertisement interval for the current APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

ipv6 initial-router-advt { **interval** *int_value* | **num-advts** *num_value* }

[**default**] **ipv6 initial-router-advt** { **interval** | **num-advts** }

default

Resets interval or num-advts to their default setting.

interval *int_value*

Specifies the time interval (in milliseocnds) when the initial IPv6 router advertisement is sent to the mobile node as an integer from 100 through 16000. Default: 3000ms
value is .

num-advts value *num_value*

Specifies the number of initial IPv6 router advertisements sent to the mobile node as an integer from 1 through 16. Default: 3

Usage

This command is used to set the advertisement interval and the number of advertisements. Using a smaller advertisement interval increases the likelihood of router being discovered more quickly when it first becomes available.

Example

The following command specifies the initial ipv6 router interval to be 2000ms:

```
ipv6 initial-router-advt interval 2000
```

l3-to-l2-tunnel address-policy

Configures the address allocation/validation policy, when subscriber L3 (IPv4/IPv6) sessions are tunneled using an L2 tunneling protocol, such as L2TP.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
l3-to-l2-tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }

default l3-to-l2-tunnel address-policy
```

default

Restores the layer 3-to-layer 2 tunnel address policy parameter to the default setting of validation with no allocation.

alloc-only

Specifies that the system locally allocates and validates subscriber addresses. Default: Disabled

alloc-validate

Specifies that the system allocates addresses when IP addresses are dynamically assigned. The system does not validate the address specified by the subscriber. Default: Disabled

no-alloc-validate

Specifies that the system does not allocate or validate subscriber addresses locally for such sessions; it passes the address between remote tunnel terminator to the mobile node. Default: Enabled

Usage

This command can be useful for MIP HA sessions tunneled from the system using L2TP tunnels, or GGSN PDP contexts of type IP tunneled using L2TP to a remote LNS.

Example

The following command configures the system to locally allocate and validate subscriber addresses:

```
l3-to-l2-tunnel address-policy alloc-only
```

loadbalance-tunnel-peers

Configures how tunnel-peers are selected for this APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

loadbalance-tunnel-peers { **balanced** | **prioritized** | **random** }

default loadbalance-tunnel-peers

default

Restores the loadbalance-tunnel-peers parameter to the default setting of random.

balanced

Tunnel-peer selection is made without regard to prioritization, but in a sequential order that balances the load across the total number of peer nodes available. Default: Disabled

prioritized

Tunnel-peer selection is made based on the priority configured for the peer. Default: Disabled

random

Tunnel-peer selection is random in order. Default: Enabled

Usage

Use this command to configure the load-balancing algorithm that defines how the tunnel-peers are selected by the APN when multiple peers are configured in the APN.

Example

The following command sets the APN to connect to tunnel-peers in a sequential order:

```
load-balancing balanced
```

long-duration-action detection

Sets the detection of a session that exceeds the long duration timer and sends notification.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
long-duration-action detection

default long-duration-action
```

default

Restores the long-duration-action parameter to its default setting of detection.

long-duration-action detection

Detects long duration sessions and sends SNMP TRAP and CORBA notification. This is the default behavior.
Default: Enabled

Usage

Use this command to detect a session that exceeds the limit set by the long duration timer.
Refer to the **timeout idle** and **timeout long-duration** commands for information on setting the long duration timer.

Example

Use the following command to enable detecting the session that exceeds the long duration timer:

```
long-duration-action detection
```

long-duration-action disconnection

Specifies what action is taken when the long duration timer expires.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
long-duration-action disconnection [ suppress-notification ] [ dormant-only ] +
```

long-duration-action disconnection

Detects a long duration session and disconnects the session after sending SNMP TRAP and CORBA notification. Default: Disabled

suppress-notifiaction

Suppress the SNMP TRAP and CORBA notification after detecting and disconnecting a long duration session. Default: Disabled

dormant only

Disconnects the dormant sessions after long duration timer and inactivity time with idle time-out duration expires. It sends the SNMP TRAP and CORBA notification after disconnecting a long duration session. Default: Disabled

Usage

Use this command to determine what action is taken when a session exceeds the limit set by the long duration timer.
Refer to the **timeout idle** and **timeout long-duration** command for information on setting the long duration timer.

Example

Use the following command to enable disconnecting sessions that exceed the long duration timer:

```
long-duration-action disconnection
```

Use the following command to disconnect the session that exceed the long duration timer without sending SNMP TRAP and CORBA notification:

```
long-duration-action disconnection suppress-notification
```

Use the following command to disconnect the session that exceed the long duration timer and also inactivity timer for idle time-out duration and send SNMP TRAP and CORBA notification:

```
long-duration-action disconnection dormant-only
```

Use the following command to disconnect the session that exceed the long duration timer and also inactivity timer for idle time-out duration without sending any SNMP TRAP and CORBA notification. If the session is idle and the session-idle-time >= inactivity time the session gets disconnected. Even if session is idle when

the long-duration timed-out and session-idle time < inactivity time the timer value is reset to idle-timeout time.

long-duration-action disconnection dormant-only suppress-notification

max-contexts

Configures the maximum number of PDP contexts (primary and secondary) that can be facilitated by the APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

max-contexts [per-subscriber secondary *secondary_ctx* **] [primary** *number* **total** *total_number* **]**

default max-contexts

default

Restores the max-contexts parameter to its default settings of:

- **primary:** 1000000
- **total:** 1000000

per-subscriber secondary *secondary_ctx*

This keyword specifies the maximum number of secondary PDP contexts that can be facilitated by the APN per primary context (per-subscriber). Subscribers can have primary PDP and secondary PDP contexts; the secondary contexts share the same IP address as the primary.
secondary_ctx is an integer from 0 through 10. Default: 10

primary *number*

This keyword specifies the maximum number of primary PDP contexts that can be facilitated by the APN. Subscribers can have primary PDP and secondary PDP contexts; the secondary contexts can be configured using the **per-subscriber secondary** keyword.
number isbe an integer value from 1 to 4000000. Default: 4000000

total *total_number*

Specifies the maximum total number of PDP contexts (primary and secondary) that can be facilitated by the APN. *total_number* can be configured to any integer value from 1 to 4000000. Default: 4000000

Usage

This parameter can be used to configure a “soft” limit on the number of PDP contexts supported by a single APN.
Soft limits are based on measurements gathered at regular short intervals (several times per minute) as opposed to measurements taken in real-time. Therefore the sampled measurement may not match the actual number of PDP contexts currently being processed. Every PDP context request received is compared against the result of the last sample. If the sample is less than the soft limit configured, the request will be processed. If it is more, the request will be rejected.

Example

The following command specifies that the maximum number of primary PDP contexts the APN can facilitate is 500,000 while the maximum total number is 750,000:

```
max-contexts primary 500000 total 750000
```

mbms bmsc-profile

Applies a configured Broadcast-Multicast Service Center (BM-SC) profile to subscribers through APN for Multimedia Broadcast Multicast Service (MBMS) support and functionality.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

mbms bmsc-profile name *bmsc_profile_name*

[default | no] mbms bmsc-profile

default

Applies the default BMSC profile to the subscribers through the APN.

no

Deletes a previously associated BM-SC profile with this APN.

name *bmsc_profile_name*

Specifies a name for the BM-SC profile already configured in BMSC configuration mode.
bmsc_profile_name is an alphanumeric string of 1 through 79 characters that may contain dots (.) and/or dashes (-).

Usage

Use this command to associate a configured BM-SC profile to use for MBMS contexts with this APN for MBMS feature support.
For more information on BM-SC profile configuration, refer to the *BMSC Profile Configuration Mode Commands* chapter.
This command also configures the specific BM-SC profile to use for Internet Group Management Protocol (IGMP) JOIN requests received from PDP contexts with this APN.

Example

Following command applies a previously configured BM-SC profile named *bm_sc_1* to an APN within the specific context.

```
mbms bmsc-profile name bm_sc_1
```

mbms bearer timeout

Configures the session timeout values for the Multimedia Broadcast Multicast Service (MBMS) bearer contexts with this MBMS APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

mbms bearer timeout { absolute | idle } *time*

[default | no] mbms bearer timeout { absolute | idle }

default

Sets the default value for the followed option for MBMS bearer context timeout.

no

Returns the timeout parameter to its default setting. If neither the absolute or idle keywords are used in conjunction with this keyword, both timeout options will be returned to their default settings.

absolute

Configures the absolute maximum time (in seconds) an MBMS bearer context may exist in any state (active or idle). Default: Disabled

idle

Default: Disabled
Configures the maximum amount of time (in seconds) an MBMS bearer context may be idle.

time

time can be any integer value between 0 and 4294967295. A time of 0 disables timeouts for this APN.
Default: 0

Usage

Use this command to limit the amount of time that an MBMS bearer context session can remain connected.

Example

The following commands enables an absolute time timeout of *60000* seconds for MBMS bearer context:

```
mbms bearer timeout absolute 60000
```

mbms ue timeout

Configures the session timeout values for the Multimedia Broadcast Multicast Service (MBMS) user equipment (UE) contexts with this MBMS APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

mbms ue timeout absolute *time*

[default | no] mbms ue timeout absolute

default

Set the default value for the followed option for MBMS UE context timeout.

no

Returns the timeout parameter to its default setting. If neither the absolute or idle keywords are used in conjunction with this keyword, both timeout options will be returned to their default settings.

absolute *time*

Configures the absolute maximum time (in seconds) an MBMS UE context may exist in any state (active or idle). *time* can be any integer value between 0 and 4294967295. A time of 0 disables timeouts for this APN. Default: 0

Usage

Use this command to limit the amount of time that an MBMS UE context session can remain connected.

Example

The following commands enables an absolute time timeout of *60000* seconds for MBMS UE context:

```
mbms bearer timeout absolute 60000
```

mediation-device

Enables the use of a mediation device and specifies the system context to use for communicating with the device.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
mediation-device [ context-name context_name ] [ delay-GTP-response ] [ no-early-PDUs ] [
no interims ] +

[ default | no ] mediation-device
```

+

Indicates that more than one of the options can be specified with a single execution of the command.

default

Changes the mediation device to no context-name configured and restores the mediation device's default properties.

no

Deletes the mediation-device configuration.

context-name *context_name*

Configures the mediation VPN context for this APN as an alphanumeric string of 1 through 79 characters that is case sensitive. If not specified, the mediation context is the same as the destination context of the subscriber. Default: The subscribers destination context.

delay-GTP-response

When enabled, delays the CPC response until an Accounting Start response is received from the mediation device. Default: Disabled

no-early-pdus

Specifies that the system delays PDUs from the MS until a response to the GGSN accounting start request is received from the mediation device. The PDUs are queued, not discarded. Default: Disabled
If "no-early-PDUs" is enabled, the chassis does not send uplink/downlink data from/to a MS until it receives the Acct-Rsp Start for the same from the mediation device. On receiving the Acct-Rsp, pending PDUs are forwarded. The chassis buffers up to two PDUs per call. As soon as the third PDU comes, the buffering is disabled and all the PDUs are forwarded for that call.
Configures the system to queue up to two PDUs until the mediation device returns a response to the system's accounting START request per 3GPP standards. On receiving the Accounting response message, the system forwards the subsequent PDUs without discarding any of the packets.

Important: For StarOS 10.0 and earlier releases, the system buffers up to four PDUs and queues or discards the remaining PDUs.

Important: For StarOS 11.0 and later releases, the system is configured so that none of the PDUs are discarded.

no-interims

Disables sending interims to the mediation server. Default: Disabled

Important: Different commands are used to disable RADIUS interims for RADIUS accounting and mediation accounting. To disable RADIUS interims for mediation accounting, use the following command: **mediation-device context-name** *context_name* **no-interims**. To disable RADIUS interims for RADIUS accounting, use the following command: **accounting-mode radius-diameter no-interims**.

Usage

This command enables mediation device support for the APN. Mediation devices can be either deep-packet inspection servers or transaction control servers.
Keywords to this command can be used in combination to each other, depending on configuration requirements.

Example

The following command enables mediation device support for the APN and uses the protocol configuration located in an system context called *ggsn1*:

```
mediation-device context-name ggsn1

mediation-device context-name ggsn1 no-interims no-early-pdus

mediation-device no-early-pdus no-interims

mediation-device no-interims no-early-pdus
```

The following command enables mediation device support for the APN and uses the protocol configuration located in the subscribers destination context:

```
mediation-device
```

mobile-ip home-agent

Configures the IP address of the home agent (HA) used by the current APN to facilitate subscriber Mobile IP sessions.

Product

GGSN, FA, P-GW

Privilege

Security Administrator, Administrator

Syntax

mobile-ip home-agent *ip_address* **[alternate]**

no mobile-ip home-agent *ip_address* **alternate**

default mobile ip home-agent

default

Restores the APN mobile-ip parameters to the default setting, no HA address defined.

no

Removes a previously configured HA address.

ip_address

Specifies the IP address of the HA expressed in IPv4 dotted-decimal notation.

alternate

Designates this Mobile IP HA as the alternate that will be used in the event of a fail-over.

Usage

If the APN is configured to support Mobile IP for all PDP contexts it is facilitating, this command specifies the IP address of the HA that is to be used.

Example

The following command configures an HA IP address of 192.168.1.15:

```
mobile-ip home-agent 192.168.1.15
```

mobile-ip mn-aaa-removal-indication

Configures the system to remove various information elements when relaying Registration Request messages to the HA.

Product

GGSN, FA, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] mobile-ip mn-aaa-removal-indication
```

default

Sets the default setting for mobile IP MN-AAA-Removal-Indication.

no

Disables this functionality. This is the default setting.

Usage

When this functionality is enabled, the MN-FA challenge and MN-AAA authentication extensions are removed when relaying a Registration Request (RRQ) to the HA.

mobile-ip mn-ha-hash-algorithm

Designates the encryption algorithm to use for Hash-based Message Authentication Code (HMAC).

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
mobile-ip mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }

default mobile-ip mn-ha-hash-algorithm
```

default

Designates the default encryption algorithm to use.

hmac-md5 | md5 | rfc-2002-md5

Default: hmac-md5
The encryption algorithms that may be used.

Usage

Provides security by encrypting the data.

Example

The following command sets encryption for md5:

```
mobile-ip mn-ha-hash-algorithm md5
```

mobile-ip mn-ha-shared-key

Configures the subscriber MobileNode-Home Agent (MN-HA) shared key.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

mobile-ip mn-ha-shared-key *key*

no mobile-ip mn-ha-shared-key

no

Disables this functionality. This is the default setting.

key

Specifies the subscriber MN-HA shared key as either an alphanumeric string or a hexadecimal number sequence beginning with "0x". The string or sequence consists of 16 to 127 characters.

Usage

Configures a shared key for the APN.

Example

The following command configures a shared key as the alphanumeric string *sfd23408imi9yn*:

```
mobile-ip mn-ha-shared-key sfd23408imi9yn
```

mobile-ip mn-ha-spi

Configures the Mobile IP Security Parameter Index (SPI).

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

mobile-ip mn-ha-spi *spi_number*

no mobile-ip mn-ha-spi

no

Disables this functionality. This is the default setting.

spi_number

Specifies the SPI as an integer from 256 through 4294967295.

Usage

Configures an SPI for the APN.

Example

The following command configures an SPI of *151111111111111111111111111111111*:

```
mobile-ip mn-ha-spi 151111111111111111111111111111111
```

mobile-ip required

Enables support for Mobile IP functionality for all PDP contexts facilitated by the current APN.

Product

GGSN, FA, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] mobile-ip required
```

default

Applies the default setting for mobile-ip for the APN. Default is disabled.

no

Disables mobile-ip for the APN.

Usage

Mobile IP functionality for IP PDP contexts is only supported at the APN-level. This command enables or disables Mobile IP support for the APN.
When Mobile IP is performed, the system authenticates the subscriber and the Mobile IP FA.
If this option is enabled, the system deletes all PDP contexts attempting to access the APN for which a Mobile IP session can not be established.

mobile-ip reverse-tunnel

Configures the system to support reverse-tunneling for Mobile IP sessions facilitated by the current APN.

Product

GGSN, FA, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] mobile-ip reverse-tunnel
```

default

Designates the default reverse tunnel for the APN. The default is enabled.

no

Disables this functionality.

Usage

Use this command to enable support for Mobile IP reverse tunneling for the APN. Reverse tunneling is enabled by default.

nai-construction

Configures the Network Access Identifier (NAI) construction parameters on a per-APN basis only, rather than by per-aaa-group when constructed NAI authentication is enabled.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

nai-construction { imsi | msisdn } [override-null-username] [encrypted password *encrypt_password* **| use-shared-secret-password | password** *password* **]**

no nai-construction

no

Disables the NAI construction at the APN level.

imsi

Enables NAI construction using IMSI for authentication for a user. GGSN constructs NAI using IMSI when no user-name is received. This is the default setting. Default: Enabled

msisdn

Enables NAI construction using Mobile Station International ISDN Number (MSISDN) for authentication for a user. GGSN constructs NAI using MSISDN when no user-name is received.

override-null-username

Enables NAI construction using IMSI/MSISDN for authentication for a user or when empty user name is received.

encrypted password

Specifies an encrypted password is to be used for this NAI-constructed user. *string* is an alphanumeric string of 0 through 63 characters.

password

Configures the authentication user-password for this NAI-constructed user. *password* is an alphanumeric string of 0 through 63 characters.

use-shared-secret-password

Specifies use of the RADIUS authentication shared secret password for this NAI-constructed user.

Usage

NAI-construction defines the behavior for construction at the APN level. If defined for a particular APN, this command works independently and overwrites the behavior of aaa constructed-nai defined at the context level for calls involving this APN.
Note that NAI construction using IMSI or MSISDN, where either no user name is received or a blank user name is received for authentication, is applicable only when NAI constructed authentication is enabled using the **aaa nai-construction authentication** command in Context Configuration Mode.

Example

The following command enables NAI-construction using IMSI as the authentication type with an encrypted password:

```
nai-construction imsi encrypted password s1289sf980333jwwdo97342
```

nbns

Configures and enables use of NetBios Name Service (NBNS) for the APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

[no] nbns { primary | secondary } *IP_address*

no

Removes/disables use of a previously configured NetBios Name Service.

primary

Designates primary NBNS server. Must be followed with an IPv4 address in dotted-decimal notation.

secondary

Designates secondary/failover NBNS server. Must be followed with an IPv4 address in dotted-decimal notation.

IP_address

Specifies the IP address in IPv4 dotted-decimal notation.

Usage

This command specifies NBNS parameters. The NBNS option is present for both pdp type IP and pdp type PPP for GGSN.
The system can be configured to use NetBios Name Service for the APN.

Example

The following command configures the APN's NetBios Name Service to primary IP 192.168.1.15.

```
nbns primary 192.168.1.15
```

nexthop-forwarding-address

Configures the next hop forwarding address for the APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

nexthop-forwarding-address *ip_address*

no nexthop-forwarding-address

no

Disables this function. This is the default setting.

ip_address

Specifies the IP address of the nexthop forwarding address in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to configure the next hop forwarding address for the APN.

Example

The following command configures the next hop forwarding address to 10.1.1.1:

```
nexthop-forwarding-address 10.1.1.1
```

npu qos

Configures an NPU QoS priority queue for packets facilitated by the APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator\

Syntax

npu qos traffic priority { best-effort | bronze | derive-from-packet-dscp | gold | silver }

default npu qos traffic priority

default

Configures the default NPU QoS traffic priority.

traffic priority { best-effort | bronze | derive-from-packet-dscp | gold | silver }

best-effort: Assigns the best-effort queue priority. This is the lowest priority.
bronze: Assigns the bronze queue priority. This is the third-highest priority.
derive-from-packet-dscp: Specifies that the priority is to be determined from the DSCP (Differentiated Services Code Point) field in the packet's TOS octet. Default: Enabled
gold: Assigns the gold queue priority. This is the highest priority.
silver: Assigns the silver queue priority. This is the second-highest priority.

Usage

This command is used in conjunction with the Network Processing Unit (NPU) Quality of Service (QoS) functionality.
The system can be configured to determine the priority of a subscriber packet either based on the configuration of the APN, or from the differentiated service (DS) field in the packet's TOS octet (representing the differentiated service code point (DSCP) value).
Refer to the *GGSN Administration Guide* for additional information on NPU QoS functionality.

Example

The following command configures the APN's priority queue to be *gold*:

```
npu qos traffic priority gold
```

outbound

Configures the APN host username and password.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
outbound { [ encrypted ] password pwd | username name }

no outbound password | username
```

no

Removes previously configured outbound information for the APN.

encrypted

The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

password *pwd*

Specifies the password to use for session authentication as an alphanumeric string of 1 through 132 characters that is case sensitive.

username *name*

Specifies the username to use for session authentication as an alphanumeric string of 1 to 127 characters that is case sensitive.

Usage

This command can be used to provide a username and password for authentication when the subscriber does not supply one in accordance with 3GPP standards. In addition, it can be used to create a PPP session when using L2TP to tunnel IP PDP contexts.
If only a username is specified using this command, the password is determined based on the setting of the **aaa constructed-nai** command in the Context Configuration mode. That command is also used to determine the password if an outbound username and password are configured for the APN when the imsi-auth keyword is specified for the **authentication** command in this mode.

Example

The following commands configures an APN username of *isp1* and a password of *secRet123*.

```
outbound username isp1

outbound password secRet123
```

p-cscf

Enables use of locally configured Proxy Call Session Control Function (P-CSCF) addresses or a Fully Qualified Domain Name (FQDN).

Product

P-GW

Privilege

Security Administrator, Administrator

Syntax

p-cscf { fqdn *fqdn* **| primary [ip** *IPv4_address* **| ipv6** *IPv6_address* **] | secondary [ip** *IPv4_address* **| ipv6** *IPv6_address* **] }**

no p-cscf { fqdn | primary [ip | ipv6] | secondary [ip | ipv6] }

no

Disables use of previously configured P-CSCF addresses or FQDN.

fqdn *fqdn*

Configures the P-CSCF FQDN server name for the APN as an alphanumeric string of 1 through 256 characters.

primary [ip*IPv4_address* **| ipv6** *IPv6_address* **]**

Specifies the primary P-CSCF address for the APN.
IPv4_address must be expressed in IPv4 dotted-decimal notation.
IPv6_address must be expressed in IPv6 colon-separated notation.

secondary [ip *IPv4_address* **| ipv6** *IPv6_address* **]**

Specifies the secondary P-CSCF address for the APN.
IPv4_address must be expressed in IPv4 dotted-decimal notation.
IPv6_address must be expressed in IPv6 colon-separated notation.

Usage

Use this command to specify the P-CSCF addresses or FQDN server name associated with this APN.

Example

The following command enables a P-CSCF with the primary IPv4 address *10.2.3.4* for the APN:

```
p-cscf primary ip 10.2.3.4
```

The following command enables a P-CSCF with FQDN server name *pcscfalias1.ind.pun.cisco.com* for the APN:

```
p-cscf fqdn pcscfalias1.ind.pun.cisco.com
```

pdp-type

Configures the type of PDP contexts that are supported by this APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
pdp-type { ipv4 [ ipv6 ] | ipv6 [ ipv4 ] | ppp }

default pdp-type
```

default

Configures the default PDP type, IPv4, for the APN.

ipv4 [ipv6]

Enables support for IPv4 PDP contexts. Also enables support for IPv6 if the IPv6 optional keyword is entered in this command. Default: Enabled

Important: Entering both IPv4 and IPv6 in either order enables support for both.

ipv6 [ipv4]

Enables support for IPv6 PDP contexts. Also enables support for IPv4 if the IPv6 optional keyword is entered in this command. Default: Disabled

Important: Entering both IPv4 and IPv6 in either order enables support for both.

ppp

Enables support for PPP PDP contexts. Default: Disabled

Usage

IP PDP context types are those in which the MS is communicating with a PDN such as the Internet or an intranet using IP. PPP PDP contexts are those in which PPP or PPP Network Control Protocol (NCP) frames from the MS are either terminated at, or forwarded by the GGSN.
If a session specifies a PDP type that is not supported by the APN, the system rejects the session with a cause code of 220 (DCH, Unknown PDP address or PDP type).

Caution: For the IPv6 calls to work, the destination context must have at least one IPv6 interface configured.

Example

The following command configures the APN to support PPP context types:

```
pdp-type ppp
```

permission

Enables the ability to use network mobility service (NEMO) functionality for the current APN.

Product

P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] permission nemo

default permission
```

no | default

Disables the ability to use NEMO functionality.

nemo

Enables the ability to use NEMO functionality.

Usage

Use this command to enable support for NEMO functionality on the APN. NEMO is disabled by default.

Example

The following command enables NEMO functionality:

```
permission nemo
```

The following command disables NEMO functionality:

```
no permission nemo
```

policy

Configures the Mobile IPv6 policy to set the action to be taken when IPv4/IPv6 subscriber packets need to be tunneled and the encapsulated packets exceed the tunnel maximum transmission unit (MTU).

Product

P-GW

Privilege

Security Administrator, Administrator

Syntax

```
policy ipv6 tunnel mtu exceed { fragment [ inner ] | notify-sender }

[ default | no ] policy ipv6 tunnel mtu exceed
```

default

IPv6: System will do a Path MTU (PMTU) discovery and send "ICMPv6 Packet Too Big" to the original sender if the subscriber packet exceeds MTU after encapsulation.
IPv4: System will do an outer IPv6 fragmentation if the packet exceeds MTU after encapsulation.

no

Disables this functionality.

ipv6 tunnel mtu exceed { fragment [inner] | notify-sender }

fragment: System will do an outer IPv6 fragmentation if the subscriber packet exceeds MTU after encapsulation.
inner:
IPv6: System will do a PMTU discovery and send "ICMPv6 Packet Too Big" to the original sender if the subscriber packet exceeds MTU after encapsulation.
IPv4: If packet will exceed tunnel MTU after encapsulation, based on DF bit and ignore-df config, the original IPv4 packet will be fragmented and then encapsulated so that it will not exceed MTU, or ICMP Error will be sent if IPv4 packet fragmentation is not allowed.
notify-sender:
IPv6: System will do a PMTU discovery and send "ICMPv6 Packet Too Big" to the original sender if subscriber packet exceeds MTU after encapsulation.
IPv4: System will do an outer IPv6 fragmentation if packet exceeds MTU after encapsulation.

Usage

This command sets the Mobile IPv6 policy for the action to be taken when IPv4/IPv6 subscriber packets need to be tunneled and the encapsulated packets exceed tunnel MTU size.

Example

The following command causes the system to do outer IPv6 fragmentation if the subscriber packet exceeds MTU after encapsulation:

```
policy ipv6 tunnel mtu exceed fragment
```

ppp

Configures the Point-to-Point Protocol (PPP) options for the current APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

ppp { **data-compression** { **protocols** *protocols* | **mode** *modes* } | **keepalive** *seconds* | **min-compression-size** *min_octets* | **mtu** *max_octets* }

default ppp { **data-compression protocols** | **keepalive** | **min-compression-size** | **mtu** }

no ppp { **data-compression protocols** | **keepalive** *seconds* | **mtu** }

default

Configures the default PPP parameters for the specified APN.

no

Resets the option specified to its default setting.

data-compression { mode *modes* **| protocols** *protocols***}**

Configures the data compression or the compression protocol to use for the APN. Default: all protocols enabled

mode *modes*: Sets the compression mode to one of the following:

- **normal**: Packets are compressed using the packet history for automatic adjustment and for best compression.
- **stateless**: Each packet is compressed individually.

protocols *protocols*: Sets the compression protocol to one of the following:

- **deflate**: DEFLATE algorithm
- **mppc**: Microsoft Point-to-Point Compression
- **stac**: STAC LZS algorithm

keepalive *seconds*

Specifies the frequency of sending the Link Control Protocol (LCP) keep alive messages. *seconds* must be either 0 or an intgeger from 5 through 14400. The special value 0 disables the keep alive messages entirely. Default: 30

min-compression-size *min_octets*

Specifies the smallest packet to which compression may be applied as an integer from 0 through 2000. Default: 128

mtu *max_octets*

Specifies the maximum transmission unit (MTU) for packets accessing the APN as an integer from 100 through 2000. Default: 1500

Important: The MTU refers to the PPP payload which excludes the two PPP octets. Therefore, an MTU of 1500 corresponds to the 3GPP standard MTU of 1502 for GTP packets with PPP payloads.

Usage

Adjust packet sizes and compression to improve bandwidth utilization. Each network may have unique characteristics such that determining the best packet size and compression options may require system monitoring over an extended period of time.

Example

The following command configures the ppp data-compression mode for the APN to be *stateless*:

```
ppp data-compression mode stateless
```

The following command configures an MTU of *500* for the APN:

```
ppp mtu 500
```

proxy-mip

Configures support for Proxy Mobile IP functionality for the APN.

Product

GGSN, FA, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] proxy-mip { required | null-username static-homeaddr }
```

default

Configures the default proxy MIP setting for the specified APN

no

Disables this functionality.

required

Default: Disabled.
Enables proxy-mip for all subscribers using this APN.

null-username static-homeaddr

Configures handling of RRQ to enable the acceptance without an NAI extension in this APN. Default: Disabled

Usage

This command requires that Proxy Mobile IP functionality be performed for all PDP contexts facilitated by the APN.
When Proxy Mobile IP is performed, the system performs subscriber authentication but not Mobile IP FA authentication. It can be configured to handling of RRQ without NAI extension in an APN.
More information about Proxy Mobile IP support for the GGSN can be found in the *GGSN Administration Guide*.

Example

The following command causes the system to support Proxy Mobile IP for all PDP contexts facilitated by the APN:

```
proxy-mip required
```

The following command will enables the accepting of RRQ without NAI extensions in this APN.

```
proxy-mip null-username static-homeaddr
```

qos negotiate-limit

Cconfigures the QoS profile to provide the peak and committed data rate limits that the GGSN assigns to the APN. The GGSN sends the QoS profile to the SGSNs in response to GTP Create/Update PDP Context requests for traffic shaping and policing functionality.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
qos negotiate-limit direction { downlink | uplink } [ qci qci_val ] [ peak-data-rate bps
[ committed-data-rate bps ] | committed-data-rate [ peak-data-rate bps ] ]

no qos negotiate-limit direction { downlink | uplink } [ qci qci_val ] }
```

no

Disables the QoS Profile for the APN.

Important: When no QoS Profile is configured, the system's default behavior is to use the information provided by the SGSN.

direction { downlink | uplink }

downlink: Apply the specified limits and actions to the downlink (to-Gn direction).
uplink: Apply the specified limits and actions to the uplink (to-Gi direction).

qci *qci_val*

qci_val is the QoS Class Identifier (QCI) for which the negotiate limit is being set. QCI ranges from 1 to 9. If no qci-val is configured, it will be handled as an undefined-qci (same as undefined-qos class).

committed-data-rate *bps*

Default: See the *Usage* section for this command
The committed data rate (guaranteed-data-rate) in bps (bits per second).
bps must be an integer from 1 through 16000000 for the downlink direction or 1 through 8640000 for the uplink direction. The value must also correspond to one of the permitted values identified the tables below. If a non-permitted value is entered for this parameter, the system rounds the value to the nearest lower supported value, except in the case where value is less than 1,000 bps. In this case, the system rounds the value to 1,000 bps. In addition, if the configured committed rate is lower than the value configured for the peak-data-rate, the system uses the configured peak rate for this parameter.

Important: System measurements for this value exclude the GTP and outer packet headers. In addition, some traffic classes have both a committed rate and a peak rate, while other traffic classes have just a peak rate. If a committed rate is not applicable (such as, the traffic class is **background** or **interactive**), an error occurs if this option is configured. If the committed-rate is applicable (such as, the traffic class is **conversational** or **streaming**), the values supplied by the SGSN are used if this option is not configured.

peak-data-rate *bps*

Default: See the *Usage* section for this command
Specifies the peak data-rate for the subscriber in bps (bits per second).
bps must be an integer from 1 through 16000000 for the downlink direction or 1 through 8640000 for the uplink direction. The value must also correspond to one of the permitted values identified in the tables below. If a non-permitted value is entered for this parameter, the system rounds the value to the nearest lower supported value, except in the case where value is less than 1,000 bps. In this case, the system rounds the value to 1,000 bps.

Usage

This command configures the APN quality of service (QoS) profile. This feature enables configuring and enforcing bandwidth limitations on individual PDP contexts of a particular traffic class. Traffic classes are defined in 3GPP TS 23.107 and are negotiated during PDP context activation. Bandwidth enforcement is configured and enforced independently for the downlink and the uplink directions.
The profile information is sent to the SGSN(s) in response to GTP Create/Update PDP Context Request messages. If the QoS profile requested by the SGSN is lower than the configured QoS profile configured, the profile requested by the SGSN is used. If the QoS profile requested by the SGSN is higher, the configured rates are used.
Note that the values for the uplink/downlink committed-data-rate and peak-data-rate parameters are exchanged in the GTP messages between the GGSN and the SGSN. Therefore, the values used may be lower than the configured values. When negotiating the rate with the SGSN(s), the system convert this to a value that is permitted by GTP as shown in the tables below.

Table 9. Permitted Values for Committed and Peak Data Rates in GTP Messages

Value (bps)	Increment Granularity (bps)
From 1000 to 63,000	1,000 (e.g 1000, 2000, 3000, ... 63000)
From 64,000 to 568,000	8,000 (e.g. 64000, 72000, 80000, ... 568000)
From 57,6000 to 8,640,000	64,000 (e.g. 576000, 640000, 704000, ... 86400000)
From 8,700,000 to 16,000,000	100,000 bps (e.g. 8700000, 8800000, 8900000, ... 16000000)

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the SGSN (such as, it accepts all of the SGSN-provided values for the PDP context.

Important: This command should be used in conjunction with the **max-contexts** command to limit the maximum possible bandwidth consumption by the APN.

Additional information on the QoS traffic shaping functionality is located in the *System Administration Guide*.
Default Values:

Example

The following command sets an uplink peak data rate of 128000 bps for QoS negotiation limit:

```
qos negotiate-limit direction uplink peak-data-rate 128000
```

qos rate-limit

Configures the action on a subscriber traffic flow that violates or exceeds the peak/committed data rate under traffic policing/shaping functionality.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
qos rate-limit direction { downlink | uplink } [ qci qci_val ] [ burst-size { bytes |
auto-readjust [ duration dur ] } ] [ exceed-action { drop | lower-ip-precedence |
transmit } [ violate-action { drop | lower-ip-precedence | shape [ transmit-when-buffer-
full ] | transmit } ] ] | [ violate-action { drop | lower-ip-precedence | shape [
transmit-when-buffer-full ] | transmit } [ exceed-action { drop | lower-ip-precedence |
transmit } ] ] +

no qos rate-limit direction { downlink | uplink } [ qci qci_val ]
```

no

Disables the QoS data rate limit configuration for the APN.

Important: When no Qos Profile is configured, the system defaults to using the information provided by the SGSN.

qos rate-limit direction { downlink | uplink }

downlink: Apply the specified limits and actions to the downlink (the Gn direction).
uplink: Apply the specified limits and actions to the uplink (the Gi direction).

qci *qci_val*

qci_val is the QoS Class Identifier (QCI) for which the negotiate limit is being set. QCI ranges from 1 to 9. If no qci-val is configured, it will be handled as an undefined-qci (same as undefined-qos class).

burst-size { *bytes* | auto-readjust [duration *dur*] }

Default: See Usage section for this command
The burst size allowed, in bytes for peak data rate and committed data rate.
bytes must be an integer from 1 through 6000000.

Important: It is recommended that the minimum value of this parameter be configured to the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the “bucket” for the configured peak-data-rate. In addition, if the committed-data-rate parameter is specified, the burst-size is applied to both the committed and peak rates.

auto-readjust [duration *dur* **]** keyword provides the option to calculate the Burst size dynamically while configuring the rate-limit. Whenever this keyword is enabled to calculate burst size, the GGSN QoS negotiated rate is enforced for this calculation.
Whenever there is a change in the rates (due to a QoS update), the burst sizes will be updated accordingly. This keyword also provides two different burst sizes. One burst size for peak rate and another for committed rate.
By default this keyword is disabled.
duration *dur* describes the duration of burst in seconds. If duration is not specified this keyword will use 1 second as default value. *dur* must be an integer between 1 through 30.

---

exceed-action { drop | lower-ip-precedence | transmit }

Default: See the *Usage* section for this command
The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

- **drop**: Drop the packet
- **lower-ip-precedence**: Transmit the packet after lowering the ip-precedence
- **transmit**: Transmit the packet

---

violate-action { drop | lower-ip-precedence | shape [transmit-when-buffer-full] | transmit }

Default: See he *Usage* section for this command
The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:
drop: Drop the packet
lower-ip-precedence: Transmit the packet after lowering the IP precedence
shape [transmit-when-buffer-full]: Enables traffic shaping and provides the buffering of user packets when subscriber traffic violates the allowed peak/committed data rate. The **transmit-when-buffer-full** keyword allows the packet to be transmitted when buffer memory is full.
transmit: Transmit the packet

+

More than one of the above keywords can be entered within a single command.

Usage

This command configures APN quality of service (QoS) data rate shaping through traffic policing/shaping. This command enables the actions on subscriber flows exceeding or violating the allowed peak/committed data rate. The shaping function also provides an enhanced function that buffers the excessive user packets and sends them to the subscriber when subscriber traffic goes below the committed or peak data rate limit.

Important: The user packet buffer function in traffic shaping is not applicable for real-time traffic.

Important: If the exceed/violate action is set to “lower-ip-precedence”, this command may override the configuration of the **ip qos-dscp** command in the GGSN Service Configuration mode for packets from the GGSN to the SGSN. In addition, the GGSN service **ip qos-dscp** command configuration can override the APN setting for packets from the GGSN to the Internet. Therefore, it is recommended that this command not be used in conjunction with this action.

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the SGSN. (It accepts all of the SGSN-provided values for the PDP context.)

Important: This command should be used in conjunction with the **max-contexts** command to limit the maximum possible bandwidth consumption by the APN.

To calculate the burst size dynamically an optional keyword **auto-readjust** [**duration** *dur*] is provided with the **burst-size** keyword. By default the burst size is fixed if defined in bytes with this command. Regardless of the rate being enforced, burst-size is fixed as set by the **burst-size** *bytes* parameter.
The **auto-readjust** [**duration** *dur*] keyword enables variable burst size depending on the rate being enforced. the system calculates burst size using a per token bucket algorithm calculation as T=B/R, where T is the time interval, B is the burst size and R is the Rate being enforced. It also provides different burst size for Peak and Committed data rate-limiting.
If the **auto-readjust** keyword is not used, a fixed burst size must be defined which will be applicable for peak data rate and committed data rate regardless of the rate being enforced.
If the **auto-readjust** keyword is provided without specifying the duration, a default duration of 1 second will be used for burst size calculation.

Example

The following command lowers the IP precedence when the committed-data-rate and the peak-data-rate are violated in uplink direction:

```
qos rate-limit direction uplink violate-action lower-ip-precedence
```

The following command buffers the excess user packets when the subscriber traffic violates the configured peak or committed data-rate bps in uplink direction. Once the peak/committed data rate for that subscriber goes below the configured limit, the system transmits the packets. It also transmits them if buffer memory is full:

```
qos rate-limit direction uplink violate-action shape transmit-when-
buffer-full
```

qos-renegotiate

This keyword is obsolete.

qos traffic-police

This command is obsolete. This functionality is now supported through **`qos negotiate-limit`** and **`qos rate-limit`** commands.

radius

This command is obsolete.

radius group

This command is obsolete.

radius returned-framed-ip-address

Sets the policy whether or not to reject a call when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
radius returned-framed-ip-address 255.255.255.255-policy { accept-call-when-ms-ip-not-supplied | reject-call-when-ms-ip-not-supplied }

default radius returned-framed-ip-address 255.255.255.255-policy
```

default

Set the policy to its default of rejecting calls when the RADIUS server does not supply a framed IP address and the MS does not supply an address.

{ accept-call-when-ms-ip-not-supplied | reject-call-when-ms-ip-not-supplied }

accept-call-when-ms-ip-not-supplied: Accept calls when the RADIUS server does not supply a framed IP address and the MS does not supply and address.
reject-call-when-ms-ip-not-supplied: Reject calls when the RADIUS server does not supply a framed IP address and the MS does not supply an address.

Usage

Use this command to set the behavior in the APN when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

Example

Use the following command to set the APN to reject calls when the RADIUS server does not supply a framed IP address and the MS does not supply an address:

```
radius returned-framed-ip-address 255.255.255.255-policy reject-call-when-ms-ip-not-supplied
```

radius returned-username

Configures the username that is returned in accounting messages. If the username is not available in the Protocol Configuration Options (PCO), the RADIUS returned username is preferred to the constructed username (imsi@apn, msisdn@apn, or outbound username).

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
radius returned-username { override-constructed-username | prefer-constructed-username }

default radius returned-username
```

default

The default value for the RADIUS returned-username is prefer-constructed-username. The constructed username (imsi@apn, msisdn@apn) will be used.

Important: If the username is available in the PCO, that username will be used regardless of the setting for this command (radius returned-username).

override-constructed-username

If the RADIUS server returns a username in the Access-Accept message and that username is not available in the Protocol Configuration Options (PCO), the new username from the RADIUS server will be used.

prefer-constructed-username

If the username is not available in the PCO, a constructed username (imsi@apn, msisdn@apn) will be used regardless of the username from the RADIUS server. This is the default.

Usage

Use this command to configure the username that is returned in accounting messages

Example

Following command sets the default value for the RADIUS returned-username is prefer-constructed-username [constructed username (imsi@apn, msisdn@apn)]:

```
default radius returned-username
```

restriction-value

Configures the level of restriction to ensure controlled co-existence of the Primary PDP Contexts.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

restriction-value *value*

[default | no] restriction-value

default | no

Default: no restriction-value
Entering either **default** or **no restriction-value** sets the internal value to zero (0) so that connection to any APN is allowed.

value

Specifies a unique number that identifies the type of network supported for primary PDP contexts facilitated by this APN. The following values are supported:

- *1*: Value used for Wireless Application Protocol (WAP) or Multimedia Messaging Service (MMS) type of networks. This corresponds to APN type public-1.
- *2*: Value used for Internet or Packet-Switched Public Data Network (PSPDN) type of networks. This corresponds to APN type public-2.
- *3*: Value used for corporate customers who use MMS. This corresponds to APN type private-1.
- *4*: Value used for corporate who do not use MMS. This corresponds to APN type private-2.

Usage

Restricts the ability to have connections to public access and certain private APNs as required by the APN configuration. Also allows co-existence of the Primary PDP Contexts in a controlled manner.
It does not restrict the total number of Primary PDP Contexts for the user. It also configures a method for preventing hackers in the public domain from using the UE as a router.
Access is provided based on the following rules:

- If *value* = 1, then PDP contexts with restriction values of 0, 1, 2, and/or 3 are allowed
- If *value* = 2, then PDP contexts with restriction values of 0, 1 and/or 2 are allowed
- If *value* = 3, then PDP contexts with restriction values of 0 and/or 1 are allowed
- If *value* = 4, then PDP contexts with no restriction values are allowed
- If **default** or **no** syntax is entered, then no PDP contexts have restriction

In the event that a Maximum APN Restriction value is received from the SGSN as part of a PDP Context Create (CPCR) or Update (UPCR) message, the GGSN allows the request based on the following matrix:

- If maximum = 0, then allow connection to any APN
- If maximum = 1, then allow APN Restriction values of 0, 1, 2, and/or 3

- If maximum = 2, then allow APN Restriction values of 0, 1 and/or 2
- If maximum = 3, the allow APN Restriction values of 0 and/or 1
- If maximum = 4, then always reject
- If maximum = anything else, then allow all APN Restriction values (1, 2, 3, and/or 4)

Refer to 3GPP 23.060 version 6.9.0 for more information.

Example

The following command sets the restriction value of the APN to *2*:

```
restriction-value 2
```

secondary ip pool

This command specifies a secondary IP pool to be used as backup pool for Network Address Translation (NAT).

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

secondary ip pool *pool_name*

no secondary ip pool

no

Removes the previous secondary IP pool configuration.

pool_name

Specifies the secondary IP pool name.
pool_name must be an alphanumeric string of 1 through 31 characters.

Usage

Use this command to configure a secondary IP pool for NAT subscribers, which is not overwritten by the RADIUS supplied list. The secondary pool configured will be appended to the RADIUS supplied IP pool list / APN provided IP pool list whichever is applicable during call setup.

Important: This command is license dependent, requiring the 600-00-7871 NAT Bypass license. Please contact your local sales representative for more information.

Example

The following command configures a secondary IP pool named *test123*:

```
secondary ip pool test123
```

selection-mode

Configures the level of verification that will be used to ensure a mobile station's subscription to use this APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
selection-mode { chosen-by-sgsn | sent-by-ms | subscribed } +

default selection-mode
```

default

Sets the default selection mode as "subscribed".

chosen-by-sgsn

Default: Disabled
The MS's subscription will not be verified and the APN will be provided by the SGSN.

sent-by-ms

Default: Disabled
The MS's subscription will not be verified and the APN will be provided by the MS.

subscribed

Default: Enabled
The MS's subscription will be verified by the SGSN.

+

More than one of the above keywords can be entered within a single command.

Usage

Use this command to specify the level of verification that will be used to ensure a MS's subscription to use this APN. This setting must mach the corresponding setting on the SGSN. If the two settings are not identical, the GGSN rejects the session with a cause code of 201 (D1H, User authentication failed).

Example

The following command specifies that the MS's subscription will not be verified and that the APN name will be supplied by the SGSN:

```
selection-mode chosen-by-sgsn
```

timeout

Configures the session timeout values for this APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

timeout { absolute | qos-renegotiate } *time*

[default | no] timeout [absolute | qos-renegotiate]

default

Set the default value for the followed option.

no

Returns the timeout parameter to its default setting. If neither the absolute or idle keywords are used in conjunction with this keyword, both timeout options will be returned to their default settings.

absolute

Configures the absolute maximum time a session may exist in any state (active or idle).

qos-renegotiate

This keyword is obsolete.

time

Default:
- absolute = 0 (Disabled)
- qos-renegotiation = 300

Measured in seconds, the time can be configured to any integer value between 0 and 4294967295.
A time of 0 disables timeouts for this APN.

Usage

Use this command to limit the amount of time that a subscriber session can remain connected or as a QoS renegotiation dampening timer.

Example

The following commands enables an absolute time timeout of *60000* seconds:

```
timeout absolute 60000
```

timeout bearer-inactivity

This command configures the bearer inactivity timer and the threshold value of the traffic (uplink + downlink) through an APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

timeout bearer-inactivity *time* **volume-threshold total** *bytes*

[default | no] timeout bearer-inactivity

default

Sets the bearer inactivity timer to disabled mode.

no

Removes the configured bearer inactivity timer values and traffic threshold limit.

time

Specifies the timeout duration in second to check inactivity on the bearer.
time must be an integer value from 3600 through 2592000.

qos-renegotiate

Configures the dampening timeout value for the QoS renegotiation (in seconds).
In the event of a QoS upgrade, the specified timeout duration will be ignored and renegotiation will start immediately.

volume-threshold total *bytes*

The keyword sets the volume threshold in bytes to check the low activity on the bearer. This total volume is the sum of the traffic in uplink and downlink directions.
bytes must be an integer value from 1 through 4294967295.

Usage

Use this command to configure the bearer inactivity timer and the threshold value of the traffic (uplink + downlink) through an APN.

Example

The following command enables the inactivity time on the bearer with a timeout duration of *7200* seconds and the total traffic volume of *256000* bytes in uplink and downlink directions as thresholds:

```
timeout bearer-inactivity 7200 volume-threshold total 25600
```

timeout emergency-inactivity

Configures the emergency session inactivity-timeout for this APN. The APN must be configured as an emergency APN for Voice over LTE (VoLTE) E911 support.

Product

All

Privilege

Security Administrator, Administrator

Syntax

timeout emergency-inactivity *seconds*

[default | no] timeout emergency-inactivity

default | no

Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified, then all are set to their default behavior.

seconds

Default: 0 (disabled)
Specifies the timeout duration, in seconds, to check inactivity on the emergency session.
seconds must be an integer value from 1 through 3600.

Usage

Use this command to set the emergency session inactivity-timeout for this APN.
At reception of an IP CAN Session Modification Request triggered by the Policy and Charging Rules Function (PCRF) for an IP-CAN (IP Connectivity Access Network) session serving an IMS emergency session that removes all PCC rules with a QCI other than the default bearer QCI and the QCI used for IMS signalling, the Policy and Charging Enforcement Function (PCEF) shall start a configurable inactivity timer (to enable PSAP Callback session). When the configured period of time expires, the PCEF shall initiate an IP-CAN Session Termination Request for the IP-CAN session serving the IMS Emergency session.
If a PCRF-Initiated IP-CAN Session Modification Request provides new PCC rule(s) with a QCI other than the default bearer QCI and the QCI used for IMS signalling, the PCEF shall cancel the inactivity timer.
Refer to the **emergency-apn** command in this chapter for additional information.

Example

The following command sets the emergency inactivity timeout duration to *450* seconds.

```
timeout emergency-inactivity 450
```

timeout idle

Configures the idle timeout duration for the long duration timer associated with a subscriber session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

timeout idle *idle_dur*

no timeout idle

no

Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified then all are set to their default behavior.

idle_dur

Default: 0
Designates the maximum duration of the session (in seconds). After expiry the system considers the session as dormant or idle and invokes the long duration timer action.
idle_dur must be an integer value in the range from 0 through 4294967295.
The special value 0 disables the timeout specified.

Usage

Use this command to set the idle time duration for subscriber session to determine the dormant session. Refer to the **long-duration-action detection** and **long-duration-action disconnection** command in this chapter for additional information.

Example

Following command sets the idle timeout duration to *450* seconds.

```
timeout idle 450
```

timeout long-duration

Configures the long duration timeout and inactivity duration for subscriber sessions.

Product

All

Privilege

Security Administrator, Administrator

Syntax

timeout long-duration *ldt_timeout* **[inactivity-time** *inact_timeout* **]**

no timeout long-duration

no

Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified then all timeouts are set to their default behavior.

ldt_timeout

Default: 0
Designates the maximum duration of the session (in seconds) before the system automatically reports/terminates the session.
Specifies the maximum amount of time (in seconds) before the specified timeout action is initiated.
ldt_timeout must be an integer value in the range from 0 through 4294967295.
The special value 0 disables the timeout specified.

inactivity-time *inact_timeout*

Specifies the maximum amount of time (in seconds) before the specified session is marked as dormant.
inact_timeout must be an integer value in the range from 0 through 4294967295.
The special value 0 disables the inactivity time specified.

Usage

Use this command to set the long duration timeout period and inactivity timer for subscriber sessions. Reduce the idle timeout to free session resources faster for use by new requests.
Refer to the **long-duration-action detection** and **long-duration-action disconnection** commands in this chapter for additional information.

Example

The following command sets the long duration timeout duration to *300* seconds and the inactivity timer for subscriber session to *45* seconds.

```
timeout long-duration 300 inactivity-time 45
```

tpo policy

Specifies the Traffic Performance Optimization (TPO) policy for the APN.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

tpo policy *tpo_policy_name*

{ default | no } tpo policy

default

Configures the default setting.
Default: Use the default TPO policy configured in the rulebase.

no

Removes the TPO policy from the APN configuration.

tpo_policy_name

Specifies the TPO policy for the APN as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify the TPO policy for the APN.

Example

The following command specifies to use the TPO policy named *tpo_policy_110*:

```
tpo policy tpo_policy_110
```

tunnel address-policy

This command specifies the address allocation/validation policy for all tunneled calls (IP-IP, IP-GRE) except L2TP calls. This means that GGSN IP address validation could be disabled for specified incoming calls.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }

default tunnel address-policy
```

default

Resets the tunnel address-policy to alloc-validate.

alloc-only

IP addresses are allocated locally and no validation is done.

alloc-validate

Default.
The VPN Manager allocates and validates all incoming IP addresses from a static pool of IP addresses.

no-alloc-validate

No IP address assignment or validation is done for calls arriving via L3 tunnels. Incoming static IP addresses are passed. This allows for the greatest flexibility.

Usage

This command supports scalable solutions for Corporate APN deployment as many corporations handle their own IP address assignments. In some cases this is done to relieve the customer or the mobile operators from the necessity of reconfiguring the range of IP addresses for the IP pools at the GGSN.
For calls coming through L2TP tunnels, the command **l3-to-l2-tunnel address policy** as defined in the APN Configuration mode, will be in effect.

Example

Use the following command to reset the IP address validation policy to validate against a static pool of address:

```
default tunnel address-policy
```

Use the following command to disable all IP address validation for calls coming through tunnels:

```
tunnel address-policy no-alloc-validate
```

tunnel gre

Configures Generic Routing Encapsulation (GRE) tunnel parameters between the GGSN and an external gateway for the APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

tunnel gre peer-address *peer_address* **local-address** *local_addr* **[preference** *num* **]**

no tunnel gre peer-address *peer_address*

no

Disables GRE tunneling for the APN.

peer-address *peer_address*

Specifies the IP address of the external gateway terminating the GRE tunnel.
peer_address must be expressed in dotted decimal notation.

local-address *local_addr*

Specifies the IP address of the interface in the destination context of the GGSN originating the GRE tunnel.
local_addr must be expressed in IPv4 dotted-decimal notation.

preference *num*

Default: 1
This option can be used to assign a preference to the tunnel.
preference can be configured to any integer value from 1 to 128.

Important: Only one GRE tunnel per APN is supported. Therefore, the preference should always be set to "1".

Usage

Subscriber IP payloads are encapsulated with IP/GRE headers and tunneled by the GGSN to an external gateway.

Example

The following command configures the system to encapsulate subscriber traffic using GRE and tunnel it from a local address of *192.168.1.100* to a gateway with an IP address of *192.168.1.225*:

```
tunnel gre peer-address 192.168.1.225 local-address 192.168.1.100
preference 1
```

tunnel ipip

Configures IP-in-IP tunnelling parameters between the GGSN and an external gateway for the APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

tunnel ipip peer-address *peer_address* **local-address** *local_addr* **[preference** *num* **]**

no tunnel ipip

no

Disables IP-in-IP tunneling for the APN.

peer-address *peer_address*

Specifies the IP address of the external gateway terminating the IP-in-IP tunnel.
peer_address must be expressed in IPv4 dotted-decimal notation.

local-address *local_addr*

Specifies the IP address of the interface in the destination context of the GGSN originating the IP-in-IP tunnel.
local_addr must be expressed in IPv4 dotted-decimal notation.

preference *num*

Default: 1
If multiple tunnels will be configured, this option can be used to assign a preference to the tunnel.
preference can be configured to any integer value from 1 to 128.

Usage

Subscriber IP payloads are encapsulated with IP-in-IP headers and tunneled by the GGSN to an external gateway.

Example

The following command configures the system to encapsulate subscriber traffic using IP-in-IP and tunnel it from a local address of *192.168.1.100* to a gateway with an IP address of *192.168.1.225*:

```
tunnel ipip peer-address 192.168.1.225 local-address 192.168.1.100
preference 1
```

tunnel ipsec

This command configures sessions for the current APN to use an Internet Protocol Security (IPSec) tunnel based on the IP pool corresponding to the subscribers assigned IP address.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] tunnel ipsec use-policy-matching-ip-pool
```

no

Disables the use of the IPSec policy that matches the IP pool that the assigned IP address relates to.

Usage

Use this command to set the APN to use an IPSec policy that is assigned to the IP pool that the subscribers assigned IP address relates to.

Example

The following command enables the use of the policy that matches the IP pool address:

```
tunnel ipsec use-policy-matching-ip-pool
```

tunnel l2tp

Configures Layer 2 Tunnelling Protocol (L2TP) parameters between the GGSN and an external gateway for the APN.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

tunnel l2tp [peer-address *lns-address* **[[encrypted] secret** *l2tp_secret* **] [preference** *num* **] [tunnel-context** *name* **] [local-address** *ip-address* **] [crypto-map** *map_name* **{ [encrypted] isakmp-secret** *crypto_secret* **}] [local-hostname** *hostname* **]**

no tunnel [peer-address *lns-address***]**

no

Disables L2TP, or secure L2TP tunneling for the APN if a specific peer-address is not specified, or, if a peer-address is specified, this keyword removes the peer-address configuration from the APN.

peer-address *lns-address*

Specifies the IP address of the LNS node that the LAC service connects to.
lns-address must be expressed in IPv4 dotted-decimal notation.

Important: A maximum of four LNS peers can be configured per APN.

encrypted

This keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

secret *l2tp_secret*

Specifies the shared secret (password) between the L2TP Access Concentrator (LAC) service (configured on the system) and the LNS node.
l2tp_secret must be an alphanumeric string of 1 through 127 characters and is case sensitive.

preference *num*

Default: 1
Specifies the preference of the tunnel if the LAC service communicates with multiple LNS nodes.
preference can be configured to any integer value from 1 to 128.

tunnel-context *name*

Specifies the name of the destination context on the system in which the LAC service(s) is configured.
name must be an alphanumeric string of 1 through 79 characters and is case sensitive.

Important: If this option is not configured, the system will attempt to determine the name of the destination context from the **ip context-name** parameter configured for the APN.

local-address *ip-address*

Specifies the IP address of an interface that is bound to a LAC service. This is a mechanism to dictate which LAC service to use to facilitate the subscriber's L2TP session.
address is the IP address of the interface in IPv4 dotted-decimal notation.

Important: If the address configured does not exist or is not bound to a LAC service, the system will automatically choose a LAC service to use.

local-hostname *hostname*

This keyword configures LAC-Hostname to be used for the communication with the LNS peer for this APN. When Tunnel parameters are not received from the RADIUS server, Tunnel parameters configured in APN are considered for the LNS peer selection. When APN Configuration is selected, local-hostname configured with the "tunnel l2tp" command in the APN for the LNS peer will be used as a LAC Hostname.

Important: For this configuration to take effect **allow aaa-assigned-hostname** command, which is used to configure LAC-Hostname based on the "Tunnel-Client-Auth-ID" attribute received from the RADIUS server, needs to be configured in the LAC Service Configuration mode.

hostname is name of the local host for the LNS peer and must be an alphanumeric string of 1 through 127 characters.
When Tunnel parameters are not received from the RADIUS Server, Tunnel parameters configured in APN will be considered for the LNS peer selection. When APN Configuration is selected, the local hostname *hostname* configured with this command in the APN for the LNS peer will be used as a LAC Hostname.

crypto-map *map_name* **{ [encrypted] secret** *crypto_secret* **}**

Configures the IPSec crypto-map policy that is to be associated with this L2TP tunnel configuration for secure L2TP.
map_name is the name of a crypto-map policy configured on the system expressed as an alphanumeric string of 1 through 127 characters and is case sensitive.
encrypted is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.
secret specifies the secret associated with the crypto-map policy. *crypto_secret* can be from 0 to 255 bytes.

Usage

This command can be used to configure the GGSN to tunnel subscriber traffic to one or more peer LNSs using L2TP or L2TP with IPSec.
When using L2TP, the system functions as a L2TP access Concentrator (LAC) and tunnels traffic to a peer L2TP Network Server (LNS). LAC functionality is supported through the configuration of LAC Services defined in destination contexts configured on the system.

When using crypt-map policies, the system functions in the same fashion as with L2TP, with the exception that the encapsulated L2TP traffic is further encrypted using IPSec. IPSec functionality is supported through the definition of crypto maps configured in the same destination context as the LAC services.
A maximum of four LNS peers can be configured per APN. If no peer is specified, the system will use the LAC Service(s) configured in the same destination context as the APN.

Example

The following command configures L2TP support for the APN. It configures the APN to tunnel traffic to an LNS with an IP address of 192.168.1.50 through a LAC service bound to an interface with an IP address 192.168.1.201 configured in a destination context on the system called pdn1. The shared secret between the system and the LNS is 5496secRet. This will be the only LNS configured so the default preference of 1 will not be changed.

```
tunnel l2tp peer-address 192.168.1.50 secret 5496secRet tunnel-context
pdn1 local-address 192.168.1.201
```

virtual-apn

Configures references (or links) to alternative APNs to be used for PDP context processing based on properties of the context. This command also configures the APN properties against which the PDP contexts are compared.It also supports roaming and visiting subscribers.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

virtual-apn { gcdr apn-name-to-be-included { Gn | virtual } | preference *priority* **apn** *apn_name* **[access-gw-address {** *ip_address* **|** *ip_address/mask* **} | bearer-access-service** *svc_name* **| cc-profile** *cc_profile_index* **[rat-type { eutran | gan | geran | hspa | utran | wlan }] | domain** *domain_name* **| mcc** *mcc_number* **mnc** *mnc_number* **[cc-profile** *cc_profile_index* **] | [msin-range from** *msin_range_from* **to** *msin_range_to* **] | [rat-type { eutran | gan | geran | hspa | utran | wlan }] | msisdn-range { from** *msisdn_start_range* **to** *msisdn_to_range* **| rat-type { eutran | gan | geran | hspa | utran | wlan } } | rat-type { eutran | gan | geran | hspa | utran | wlan } | roaming-mode { home | roaming | visiting }] }**

default virtual-apn gcdr apn-name-to-be-included

no virtual-apn preference *priority*

---

default

The virtual APN name is sent in G-CDRs.

---

no

Removes a previously configured “virtual” APN.

---

gcdr apn-name-to-be-included { *gn* **|** *virtual* **}**

If **virtual** APN to be used is configured, the virtual APN name is sent in G-CDRs. Provides an option to either send the virtual APN name or the Gn APN name (that comes from the SGSN) in G-CDRs.
Gn: the APN received in the Create PDP Context Request message from SGSN.
virtual: the APN selected by the GGSN/P-GW. This is the default.

---

preference *priority*

Specifies the order in which the referenced APNs are compared by the system.
priority specifies the order and can be configured to any integer value from 1 (highest priority) to 1000 (lowest priority).

---

apn *apn_name*

Specifies the name of an alternative APN configured on the system that is to be used for PDP contexts with matching properties.
apn_name is the name of the alternative APN expressed as an alphanumeric string of 1 through 62 alphanumeric characters and is case insensitive. It may also contain dots (.) and/or dashes (-).

access-gw-address { *ip_address* | *ip_address/mask* }

Specifies the Access gateway (SGSN/SGW/Others) address for the virtual APN.
ip_address is an IP address entered in IPv4 dotted-decimal or IPv6 colon-separated notation.
ip_address/mask is the IP address in IPv4 dotted-decimal or IPv6 colon-separated notation with network-host mask separation.

bearer-access-service *svc_name*

Specifies the Bearer Access Service name for the virtual APN. This service name is unique across the context.
svc_name is an alphanumeric string of 1 through 63 characters.

cc-profile *cc_profile_index*

Specifies the APN for charging characteristics (CC)-profile index.
cc_profile_index is an integer from 1 to 15.

domain *domain_name*

Specifies the subscriber's domain name (realm).
domain_name must be an alphanumeric string of 1 through 79 characters, is case sensitive and can contain all special characters.

mcc *mcc_number*

Specifies the mobile country code (MCC) portion of the PLMN's identifier.
mcc_number is the PLMN MCC identifier and can be configured to any 3-digit integer value between 100 and 999.

mnc *mnc_number*

Specifies the mobile network code (MNC) portion of the PLMN's identifier.
mnc_number is the PLMN MNC identifier and can be configured to any 2- or 3-digit integer value between 00 and 999.

msin-range{ from *msin_range_from* **to** *msin_range_to*| **rat-type { eutran | gan | geran | hspa | utran | wlan } }**

Specifies the APN for this IMSI MSIN range or the radio access technology (RAT) type.
msin_range_from is the start prefix of the IMSI MSIN range and can be configured between 0 and 9999999999.
msin_range_to is the end prefix of the IMSI MSIN range and can be configured as a string of size 1 to 10 digits between 0 and 9999999999.
msin-range should follow the following rules

- Start prefix (such as *msin_range_from*) and end prefix (such as *msin_range_from*) must be of the same length.
- Total length of mcc + mnc + msin-range <= 15 digits.
- For a given combination of mcc + mnc + msin-range (start-end prefix), overlapping range is not allowed.

rat-type is the type of the radio access technology based on which the APN would be specified.

msisdn-range from *msisdn_start_range* **to** *msisdn_to_range*

Specifies the APN for this MSISDN range.
msisdn_start_range is the starting MSISDN number which a string of size 2 to 15 and its value ranges between 00 and 999999999999999.
msisdn_to_range is the ending MSISDN number which is also a string of size 2 to 15 and its value ranges between 00 and 999999999999999.

rat-type { eutran | gan | geran | hspa | utran | wlan }

is the type of the radio access technology based on which the APN would be specified. The available options include:

- eutran
- gan
- geran
- hspa
- utran
- wlan

roaming-mode { home | roaming | visiting }

Supports separate PDP context processing for roaming, visiting, and home subscribers. It supports separate rule type along with domain, imsi, and sgsn-address types.

Usage

This command simplifies the configuration process for mobile operators allowing them to provide subscribers with access to a large number of packet data networks, characterized by APN templates, while only having to configure a small number of APNs on the HLR.
Each "virtual" APN is a reference, or a link, to an alternate APN configured on the system. Each reference is configured with a rule that subscriber PDP contexts are compared against and a priority that dictates the comparison order. The references works as follows:
1. A Create PDP Context Request message is received by the GGSN. The message specifies an APN configured in the HLR.
2. The GGSN determine whether its own matching APN configuration contains "virtual" APN references.
3. The system determines the priority of the references and compares the associated information pertaining to the PDP context against the configured rules.
4. If the rule matches, the parameters in the APN specified by the reference are applied to the PDP context. If not, the rules in the reference with the next highest priority are compared against the PDP context. This occurs until a match is found. If none of the references match, then the parameters within the current APN are applied to the PDP context.
The GGSN supports a maximum of 1023 Virtual APN mapping configurations in a system. A single Gn APN can be configured with up to 1000 mapping rules. Multiple Gn APNs are supported - each requiring Virtual APN mapping configurations. The limit imposed is that the total virtual APN mappings across all Gn APNs should not exceed 1023.
The functionality provided by this command can also be used to restrict access to particular APNs. To restrict access based on a particular rule (either domain name or mobile country code/mobile network code), the "virtual" APN reference should refer to an APN that not is configured on the system and contain the desired rule. All PDP contexts matching the configured rule would then be denied with a reason code of 219 (DBH), Missing or Unknown APN.

Example

The following commands configure two "virtual" APNs, priority 1 references the *bigco* APN with a domain rule of *bigco.com*, priority 2 references the *bigtown* APN with a mobile country code rule of *100* and a mobile network code rule of *50*.

```
virtual-apn preference 1 apn bigco domain bigco.com

virtual-apn preference 2 apn bigtown mcc 100 mnc 50 msin-range from
4000000000 to 4999999999

virtual-apn preference 3 apn bigco.com sgsn-address 192.168.62.2

virtual-apn preference 4 apn bigco.co.kr sgsn-address 192.168.60.2/24
```

Chapter 24
APN Profile Configuration Mode

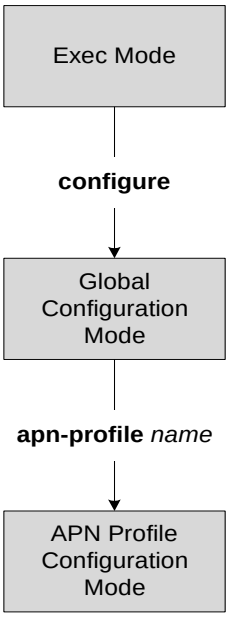
The APN Profile configuration mode defines a set of parameters controlling the SGSN or MME behavior when a specific APN is received or no APN is received in a Request. An APN profile is a key element in the Operator Policy feature and an APN profile is not used or valid unless it is associated with an APN and this association is specified in an operator policy (see the *Operator Policy Configuration Mode Commands* chapter elsewhere in this guide).

Essentially, an APN profile is a template that consists of a set of APN-specific commands that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the set of commands in the associated APN profile will be applied. The same APN profile can be associated with multiple APNs and multiple operator policies.

The SGSN and the MME each support a total of 1,000 APN profile configurations per SGSN/MME; up to 50 APN profiles can be associated with a single operator policy. For additional SGSN limit information, refer to the *Engineering Rules* appendix in the *SGSN Administration Guide*.

When this mode is accessed, the command prompt should resemble:

```
[local]asr5000(apn-profile-<profile_name>)#
```



address-resolution-mode

Identifies the address resolution mode for this APN profile. This command is specific to the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
address-resolution-mode { fallback-for-dns | local }

default address-resolution-mode
```

default

Resets the configuration to the default value; i.e. **fallback-for-dns**.

fallback-for-dns

Instructs the system to try DNS resolution. If the DNS query fails, the SGSN will use locally configured addresses, if they have been configured.
Default: enabled

local

Instructs the system to only use locally configured addresses and not to use DNS query.
Default: disabled

Usage

Use this command to specify the DNS query or local address resolution for this APN profile.

Example

The following command sets the address resolution mode to use local addresses *only if* the DNS query fails:

```
address-resolution-mode fallback-for-dns
```

apn-resolve-dns-query

Command enables the SGSN to send Straightforward Name Authority Pointer (SNAPTR) type DNS query for APN resolution on a per APN basis.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
apn-resolve-dns-query snaptr

remove apn-resolve-dns-query snaptr
```

remove

Removes the DNS SNAPTR function from the configuration.

Usage

SNAPTR filters based on the EPC-capability of the user equipment (UE). Use this command to enable SNAPTR type DNS query for APN resolution for 3G subscribers with EPC subscription. Configuration in this mode promotes control of this feature per APN.
When this functionality is enabled, an SGSN using Gn/Gp interfaces can optionally select a PGW while activating a context if the subscriber is EPS capable. This supports EPS-based mobility if the subscriber is anchored at the PGW. At PDP Context Activation, the SGSN will use the UE capability as input to select the GGSN or PGW. SNAPTR DNS query allows for PGW resolution.
By default, this functionality is not enabled.

Example

Enable the SGSN to select a PGW during APN resolution:

```
apn-resolve-dns-query snaptr
```

cc

Configures the charging characteristics (CC) for this APN profile.

Product

SGSN, S-GW

Privilege

Security Administrator, Administrator

Syntax

cc { local-value-for-scdrs behavior *bit_value* **profile** *index_bit* **| prefer { hlr-value-for-scdrs | local-value-for-scdrs } }**

remove cc { local-value-for-scdrs | prefer }

remove

Removes the charging characteristics configuration from this APN profile.

local-value-for-scdrs behavior *bit_value* **profile** *index_bit*

Sets the value of the behavior bits and profile index for the charging characteristics for S-CDRs locally, when the Home Location Register (HLR) does not provide these values.
If the HLR provides the charging characteristics with behavior bits and profile index, and the operator wants to ignore what the HLR provides, then specify the **prefer local-value-for-scdrs** keyword with this command.
bit_value: must be a hexadecimal value between 0x0 and 0xFFF.
index_bit: must be an integer from 1 through 15.
Some of the index values are predefined according to 3GPP standard:

- **1** for hot billing
- **2** for flat billing
- **4** for prepaid billing
- **8** for normal billing

Defaults: *bit_value* = 0x0; *index_bit* = 8

prefer { hlr-value-for-scdrs | local-value-for-scdrs }

Specify what charging characteristic settings the system will use for S-CDRs.

- **hlr-value-for-scdrs**: instructs the system to use charging characteristic settings received from the HLR for S-CDRs.
- **local-value-for-scdrs**: instructs the profile preference to only use locally configured/stored charging characteristic settings for S-CDRs.

Default: **hlr-value-for-scdrs**

Usage

Use this command to specify the charging characteristic for S-CDRs -- either from the HLR or locally from the SGSN.

These charging characteristics parameters for S-CDRs and M-CDRs are also configurable in the Call-Control Profile configuration mode. When CC parameters are specified in both types of profiles, then:

- For generation of M-CDRs, the parameters configured in the Call-Control Profile configuration mode will take precedence.
- For generation of S-CDRs, the parameters configured in the APN Profile configuration mode will take precedence.

Example

The following command configures the APN profile to instruct the SGSN not to use charging characteristic settings received from the HLR for S-CDR generation:

```
cc prefer hlr-value-for-scdrs
```

description

Defines a descriptive string relevant to the specific APN profile.

Product

MME, SGSN, S-GW

Privilege

Security Administrator, Administrator

Syntax

description *description*

remove description

remove

Removes the configured description from this APN profile.

description

Specifies a description for this APN profile as an alphanumeric string of 1 through 100 characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotation marks (“).

Usage

Define information that identifies this particularly APN profile.

Example

Indicate that APN profile *apnprof1* is to be used for customers in Saudi Arabia and that the profile was created on April 10th of 2010:

```
description “apnprof1 defines APNs for customers in Saudi Arabia
(4/10/10).”
```

direct-tunnel

Defines the permission for direct tunnel establishment by GGSNs. This command is specific to the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
direct-tunnel not-permitted-by-ggsn

remove direct-tunnel
```

remove

Removes the direct tunnel establishment configuration from this APN profile.

not-permitted-by-ggsn

Specifies that a direct tunnel is not permitted by the GGSN when resolved by this APN.
Default: disabled.

Usage

Use this command to enable/disable the permission for establishment of direct tunnels between an RNC and a GGSN.

Example

The following command instructs the SGSN not to permit establishment of a direct tunnel with a GGSN:

```
direct-tunnel not-permitted-by-ggsn
```

dns-extn

Takes an offset group of digits from the MSISDN and appends the digits to the DNS query string to create a new APN intended to assist roaming subscribers to use the local GGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

dns-extn { charg-id { binary | decimal | hexadecimal } | lac-rac | msisdn start-offset *start_digits* **end-offset** *end-digits* **| rnc-id [charg-id { binary | decimal | hexadecimal }] }**

remove dns-extn { charg-id | lac-rac | msisdn | rnc-id [charg-id] }

charg-id { binary | decimal | hexadecimal }

Instructs the SGSN to take the profile index value of the charging characteristics, from the PDP subscription record (selected during APN selection) and include the profile index value in the APN name prior to sending out DNS queries. The operator can also specify the format (binary, decimal or hexadecimal) for the CC information to be included.

lac-rac

Enables the SGSN to append geographical information to the APN string that is being sent in the DNS query. This information is used during the DNS query process to select the geographically closest GGSN.

msisdn start-offset *start_digits* **end-offset** *end-digits*

Defines an offset group of digits from the MSISDN and appends the digits to create a new APN DNS query string that is intended to assist roaming subscribers to use the local GGSN.

- *start_digits* is an integer from 1 through 14 that identifies the position of the first digit in the MSISDN to start the offset.
- *end-digits* is an integer from 2 through 15 that identifies the position of the last digit in the MSISDN to be part of the offset.

rnc-id [charg-id { binary | decimal | hexadecimal }]

Instructs the SGSN to include the ID of the calling RNC in the APN DNS query string. Optionally, the profile index value of the charging characteristics can be inserted into the APN name prior to sending out DNS queries. As well, the operator can specify the format (binary, decimal or hexadecimal) for the CC information to be included.

Usage

With this command, the APN in the DNS query string, used for querying the GGSN address, can be appended with additional information, such as

- digits from the MSISDN
- LAC/RAC info

- RNC-ID
- profile index from the charging characteristics information (SCHAR)

This additional information allows some customization of the DNS query string to facilitate selecting a specific (usually local or nearest) GGSN.
For example, roaming subscribers using a specific APN may want to be directed to a specific GGSN. This can be achieved by having an operator policy for roaming subscribers associated with an APN profile that includes a configuration specifying certain digits, from the MSISDN or geographical information from the LAC/RAC, be appended to the APN. This is then used as the DNS query string.
In addition, the operator must configure appropriate DNS entries to enforce the selection of the required GGSN. After appending the MSISDN digits to the DNS query string, the string will have the form: `ni.<digits>.mnc*.mcc*.gprs`. After appending the LAC/RAC information to the DNS query string, the string will have the form: `<apn_network_id>.racAAAA.lacBBBB.<apn_operator_id>` , where the AAAA and BBBB are Hex-coded digits (less than 4 significant digits and one or more zero ("0") digits will be inserted to the left side of the Hex to fill the 4-digit coding).
After appending the charging characteristic (SCHAR) information, the DNS string will take the following form: `<apn_network_id>.<profile_index>.<apn_operator_id>`. The profile index in the following example has an integer value 10: `quicknet.com.uk.1010.mnc234.mcc027.gprs`.
If the RNC-ID information is configured to be a part of the APN name, and if inclusion of the profile index of the charging characteristics information is also enabled before the DNS query is sent, the profile index is included after the included RNC-ID and the DNS APN name will appear in the following form: `<apn_network_id>.<rnc_id>.<profile_index>.<apn_operator_id>`.
Once the DNS extension is defined, the selected extension is applicable when either the wildcard APN feature or the default APN feature are configured and used.
The information is appended to the DNS query and the actual APN string sent to the GGSN will not be modified in any way.

Example

A sample MSISDN is '112233445566778' and a sample APN NI (network identifier) is 'wap98.testnetz.ca'. The following command instructs the SGSN to create a new APN with digits pulled from the MSISDN and appended to the APN:

```
msisdn start-offset 3 end-offset 9
```

The resulting APN DNS query string would have appended 7 digits (2233445)to the APN NI so that it would appear something like `wap98.testnetz.ca.2233445.MNC009.MCC262.GPRS`
Enable inclusion of geographical information in the APN string used for the DNS query to locate the closest GGSN:

```
lac-rac
```

In the following example, the DNS query for a subscriber using RNC 0321 with the profile index of value 8 would appear as: `quicknet.com.uk.0321.1000.mnc234.mcc027.gprs`

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

gateway-address

Configures the IPv4 or IPv6 address of the GGSN supporting the APN associated with this APN profile. Also, use this command to create a secondary pool of GGSNs. This command is specific to the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gateway-address *ip_address* **{ priority** *priority* **| weight** *weight* **[secondary-pool] }**

no gateway-address *ip_address*

no

Disables the GGSN address configured in this APN profile.

ip_address

Specifies the IP address for the GGSN in IPv4 dotted-decimal or IPv6 colon-separated notation.

priority *priority*

Specifies the priority, for the configured GGSN address, to be considered during address selection. If the highest priority GGSN fails to respond, the next priority level GGSN is selected. *priority* is an integer from 1 through 100. Note that the lower integer has the higher priority, so that 1 is the highest priority.

weight *weight* **[secondary-pool]**

Specifies the weight (importance) assigned to a GGSN to facilitate load balancing. *weight* is an integer from 1 to 100.
If a weight is assigned to an address, then load balancing (of primary CPC requests) depends on the weight value. For example:

```
GGSN1 172.16.130.1 weight 30 and GGSN2 172.16.130.3 weight 70
```

With this configuration, 30% of the activation requests for this APN will go to GGSN1 and 70% of the requests will go to GGSN2. Also note that the sum of the weights does not need to be 100. The calculation of weight percentiles is carried out proportionately, so the following configuration will also yield the same 30% - 70% results:

```
GGSN1 172.16.130.1 weight 6 and GGSN2 172.16.130.3 weight 14
```

secondary-pool

This optional keyword allows the operator to enable multiple GGSN pools by assigning the GGSN to a secondary pool of GGSNs. The selection algorithm for GGSNs in a secondary pool is weight-based.

Usage

Use this command to define priority or load balancing to be applied during GGSN selection. A maximum of 16 GGSN address can be configured for this APN profile.
Also use this command to setup GGSN pools - primary and secondary pools with up to 16 GGSNs in each pool. By default, GGSNs will always be selected from the primary pool. However, working in tandem with the **ggsn-fail-retry-timer** command configuration (SGTP service configuration mode) which enables the local DNS feature, some of the primary GGSNs can be temporarily blacklisted if they become unavailable or overburdened.

Example

Set a GGSN address with a secondary priority level:

```
gateway-address 123.123.123.2 priority 2
```

Add a GGSN to the secondary GGSN pool and define selection weighting of 7th:

```
gateway-address 198.168.138.8 weight 7 secondary-pool
```

gtp

Enables or disables the GTPC private extension for the Overcharging Protection feature. This command is specific to the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ remove ] gtp private-extension loss-of-radio-coverage send-to-ggsn [ send-to-peer-sgsn
]
```

remove

Disables the inclusion of the GTPC private extension, thereby disabling the Overcharging Protection feature.

private-extension loss-of-radio-coverage send-to-ggsn

Instructs the SGSN to set a proprietary GTPC private extension (in the LORC Intimation IEs) in the event of loss of radio coverage (LORC). These private extensions are only understood by a GGSN with an Overcharging Protection license.
The mandatory **loss-of-radio-coverage send-to-ggsn** keyword set instructs the SGSN to forward the private extension flag to the GGSN in the event of a loss of radio coverage (LORC).

send-to-peer-sgsn

This optional keyword instructs the SGSN to also forward the LORC private extension to the peer SGSN.

Usage

gtp private-extension is one of the two commands required to enable the Overcharging Protection feature. The second command sets the RANAP cause code in the Iu Release to enable the SGSN to detect the LORC state of the MS/UE. This second command is configured in the IuPS service and is explained in the *IuPS Service Configuration Mode* chapter.
When there is a loss of coverage and the Overcharging Protection feature is enabled with the **gtp private-extension** command, the SGSN includes the proprietary private extension in the GTP LORC Intimation IE messages. This LORC IE is also included in UPCQ, DPCQ, and SGSN Context Response GTP messages. Refer to the *SGSN Administration Guide* for additional information regarding the Overcharging Protection feature.

Example

Use the following command to have the SGSN send the GGSN the GTPC private extension in the LORC Intimation IE:

```
gtp private-extension loss-of-radio-coverage send-to-ggsn
```

idle-mode-acl

Configures a group of access control lists (ACLs) that define rules to apply to downlink data destined for UEs in an idle mode.

Product

S-GW

Privilege

Administrator

Syntax

[remove] idle-mode-acl { ipv4 | ipv6 } access-group *acl_name*

remove

Removes the specified ACL name from the access group.

{ ipv4 | ipv6 } access-group *acl_name*

Specifies the ACL type to add to the access group.

- **ipv4**: Specifies that an IPv4 ACL is being added to the access group.
- **ipv6**: Specifies that an IPv6 ACL is being added to the access group.

access-group *acl_name* specifies the name of the ACL being added to the access group as an existing IPv4 or IPv6 ACL name expressed as an alphanumeric string of 1 through 47characters.

Usage

Use this command to create a group of ACLs that contain rules to apply to data sent to UEs that are currently in idle mode.
IPv4 ACLs are configured through the Context Configuration Mode using the **ip access-list** command.
IPv6 ACLs are configured through the Context Configuration Mode using the **ipv6 access-list** command.

Example

The following command configures the APN profile to use an IPv4 ACL named *acl-3-permit* to apply rules to downlink data sent to UEs that are currently in idle mode:

```
idle-mode-acl ipv4 access-group acl-3-permit
```

ip

Defines the IP parameters for this APN profile.

Product

SGSN, S-GW

Privilege

Administrator

Syntax

```
ip { qos-dscp { { downlink | uplink } { background forwarding | conversational forwarding
| interactive traffic-handling-priority priority forwarding | streaming forwarding } + }
| source-violation { deactivate [ all-pdp | exclude-from accounting | linked-pdp |
tolerance-limit } | discard [ exclude-from-accounting ] | ignore }

default ip { qos-dscp [ downlink | uplink ] | source-violation }

no ip qos-dscp { downlink | uplink } { background | conversational | interactive |
streaming } +
```

Important: All parameters not specifically configured will be included in the configuration with default values.

default

Resets the configuration to the default values.

no

Disables the specified IP QoS-DSCP mapping.

qos-dscp

Configures the Differentiated Services Code Point (DCSP) marking to be used for sending packets of a particular 3GPP QoS class.

downlink | uplink

Configures the packets for either downlink (network to subscriber) or uplink (subscriber to network) direction. **downlink** and **uplink** configuration must include one or more of the following:

- **background** - Configures the DSCP marking to be used for packets of sessions subscribed to 3GPP background class. Must be followed by a DSCP marking
- **conversational** - Configures the DSCP marking to be used for packets of sessions subscribed to 3GPP conversational class. Must be followed by a DSCP marking
- **interactive** - Configures the DSCP marking to be used for packets of sessions subscribed to different traffic priorities in the 3GPP interactive class. Must be followed by a traffic handling priority (THP): 1, 2, or 3.
- **streaming** - Configures the DSCP marking to be used for packets of sessions subscribed to 3GPP streaming class. Must be followed by a DSCP marking

DSCP marking options

Downlink and uplink must include a DSCP forwarding marking; supported options include:

- af11 - Designates use of Assured Forwarding 11 PHB
- af12 - Designates use of Assured Forwarding 12 PHB
- af13 - Designates use of Assured Forwarding 13 PHB
- af21 - Designates use of Assured Forwarding 21 PHB
- af22 - Designates use of Assured Forwarding 22 PHB
- af23 - Designates use of Assured Forwarding 23 PHB
- af31 - Designates use of Assured Forwarding 31 PHB
- af32 - Designates use of Assured Forwarding 32 PHB
- af33 - Designates use of Assured Forwarding 33 PHB
- af41 - Designates use of Assured Forwarding 41 PHB
- af42 - Designates use of Assured Forwarding 42 PHB
- af43 - Designates use of Assured Forwarding 43 PHB
- be - Designates use of Best Effort forwarding PHB
- ef - Designates use of Expedited Forwarding PHB

Forwarding defaults for both uplink and downlink are:

- conversational - ef;
- streaming - af11;
- interactive 1 - ef;
- interactive 2 - af21;
- interactive 3 - af21;
- background - be

source-violation

Configures settings related to IP source-violation detection with one of the following criteria:

- **deactivate** - deactivate the PDP context with one of the following conditions:
- **all-pdp** - deactivates all PDP context of the MS/UE. Default is to deactivate errant PDP contexts.
- **exclude-from-accounting** - excludes packets having an invalid source IP address from the statistics used in the accounting records.
- **linked-pdp** - deactivate all associated pdp contexts (primary and secondary). Default is to deactivate errant pdp context.
- **tolerance-limit** - Configures maximum number of allowed IP source violations before the session is deactivated.
- **discard** - discard errant packets, can include the following option:
- **exclude-from-accounting** - excludes packets having an invalid source IP address from the statistics used in the accounting records.
- **ignore** - ignore checking of packets for MS/UE IP source violation.

Usage

This command configures a range of IP functions to be associated with the APN profile; such as:

- SGSN/S-GW action in response to detected IP source violations,
- DSCP marking for downlink and uplink configuration per traffic class,
- QoS class diffserv code.

Example

The following command configures the APN profile to instruct the SGSN or S-GW not to check incoming packets for IP source violation information:

```
ip source-violation ignore
```

pdp-data-inactivity

Configures the APN profile regarding PDP data inactivity. This command is specific to the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
pdp-data-inactivity { action { deactivate [ all-pdp | linked-pdp ] | detach-when { all-
pdp-inactive | any-pdp-inactive } } | timeout minutes minutes }

default pdp-data-inactivity { action | timeout }

no pdp-data-inactivity timeout
```

default

Resets the APN Profile configuration to the default values for PDP data-inactivity.

no

Disables the timeout feature of the PDP data-inactivity configuration for this APN profile.

action

Defines the action to be taken if PDP data-inactivity occurs:

- **deactivate** - defines which PDP context should be deactivated:
- **all-pdp** - deactivates all PDP contexts.
- **linked-pdp** - deactivates only linked PDP contexts.
- **detach-when** - defines the condition that warrants a detach:
- **all-pdp-inactive** - detach when all PDP contexts are inactive.
- **any-pdp-inactive** - detach when any PDP context is inactive.

timeout minutes *minutes*

Specifies the inactivity timeout in minutes. *minutes:* is an integer from 1 through 1440. Note that even though the timeout is set for minutes, the configuration displays in seconds.

Usage

Use this command to define how the SGSN will handle a situation where the PDP is not fully active. Repeat the command, as needed, to configure more than one keyword-controlled function.

Example

Use the following command to have the SGSN deactivate all PDP contexts associated with the APN when it detects the PDP is inactive:

```
pdp-data-inactivity action deactivate all-pdp
```

Use the following command to have the SGSN wait *2* minutes after detecting PDP data inactivity:

```
pdp-data-inactivity timeout minutes 2
```

pdp-type-ipv4v6-override

Configure the PDP type to use, per APN, if dual PDP type addressing is not supported by the network and the MS/UE requests the IPv4v6 PDP type.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
pdp-type-ipv4v6-overrride { ipv4 | ipv6 }

remove pdp-type-ipv4v6-overrride
```

remove

Deletes the override configuration and reverts to the default behavior so the SGSN ignores the IPv4v6 request and sends IPv4 to the GGSN.

ipv4

Configures IPv4 as the PDP type to send towards the GGSN when overriding the dual PDP type addressing requested by the MS/UE.

ipv6

Configures IPv6 as the PDP type to send towards the GGSN when overriding the dual PDP type addressing requested by the MS/UE.

Usage

This command configures the SGSN to send either IPv4 or IPv6 towards the GGSN when the MS/UE requests PDP type as IPv4v6 but either the SGSN or the RNC is not configured to support dual PDP type.

Example

Use this command to configure the SGSN to always send IPv6, for the PDP type, to the GGSN when overriding a dual PDP type address request from the MS/UE:

```
pdp-type-ipv4v6-override ipv6
```

pgw-address

Configures the IPv4 or IPv6 address of the P-GW supporting the APN associated with this APN profile. This command is specific to the MME.

Product

MME

Privilege

Administrator

Syntax

pgw-address *ip_address* **[s5-s8-protocol pmip] [weight** *weight* **]**

no pgw-address *ip_address*

no

Disables the P-GW address configured in this APN profile.

ip_address

Specifies the IP address for the P-GW in IPv4 dotted-decimal or IPv6 colon-separated notation.

s5-s8-protocol pmip

Configures the S5-S8 protocol for the gateway.

weight *weight*

Specifies the weight (importance) assigned to the addressed P-GW for load balancing. *weight* is an integer from 1 through 100.
If a weight is assigned to an address, then load balancing (of primary CPC requests) depends on the weight value. For example:

```
pgw-address 172.16.130.1 weight 30 and pgw-address 172.16.130.3 weight 70
```

With this configuration, 30% of the activation requests for this APN will go to he 130.1 address and 70% of the requests will go to 130.3 address. Also note that the sum of the weights does not need to be 100. The calculation of weight percentiles is carried out proportionately, so the following configuration will also yield the same 30% - 70% results:

```
pgw-address 172.16.130.1 weight 6 and pgw-address 172.16.130.3 weight 14
```

Usage

Use this command to define load balancing to be applied during P-GW selection. A maximum of 16 P-GW addresses can be configured for this APN profile.

Example

The following command configures the P-GW IP address for this APN profile as *10.2.3.4*:

```
pgw-address 10.2.3.4
```

qos apn-ambr

Configures the APN-AMBR (aggregate maximum bit rate) that will be stored in the Home Subscriber Server (HSS). This command is specific to the MME.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

qos apn-ambr max-ul *mbr-up* **max-dl** *mbr-dwn*

remove qos apn-ambr

remove

Removes the APN-AMBR changes from the configuration for this APN profile.

max-ul *mbr-up* **max-dl** *mbr-dwn*

Defines the maximum bit rates for uplink (subscriber to network) and downlink (network to subscriber) traffic.
mbr-up is an integer from 0 through 1410065408.
mbr-dwn is an integer from 0 through 1410065408.

Usage

Use this command to define the MBR that will be enforced by the P-GW for both uplink and downlink traffic shaping.

Example

```
qos apn-ambr max-ul 24234222 max-dl 23423423
```

qos class

Configures local values for the traffic class (TC) parameters for the quality of service (QoS) configured for this APN profile.

Important: To enable any of the values/features configured with this command, the **qos prefer-as-cap** configuration (also in the APN profile configuration mode) must be set to either **local** or **both-hlr-and-local**.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

qos class { background | conversational | interactive | streaming } [*qualif_option* **]**

remove qos class { background | conversational | interactive | streaming } [*qualif_option* **]**

remove

Removes previously defined values for the specified option or for an entire class if a qualifying option is not included in the command.

background

Selects the background traffic class. This 'best-effort' class manages traffic that is handled as a background function, like email, where time to delivery is not a key factor. The selection of background traffic class can be refined with the addition of one of the following qualifying options:

- **all-values**
- **arp**
- **mbr-down**
- **mbr-map-down**
- **mbr-map-up**
- **mbr-up**
- **residual-bit-error-rate**
- **sdu**

All qualifying options are explained below.

conversational

Selects the 'real-time' conversational traffic class of service, which has the most stringent time requirements of the four classes and is typically reserved for voice traffic. The section of the conversational traffic class can be refined with the addition of one of the following qualifying options:

- **all-values**

- **arp**
- **gbr-down**
- **gbr-up**
- **mbr-down**
- **mbr-map-down**
- **mbr-map-up**
- **mbr-up**
- **min-transfer-delay**
- **residual-bit-error-rate**
- **sdu**

All qualifying options are explained below.

---

interactive

Selects interactive traffic class of service. This class is characterized by a request/response pattern (someone sends data and then waits for a response) which requires the preservation of the data but delivers on a 'best-effort' model. The section of the interactive traffic class can be refined with the addition of one of the following qualifying options:

- **all-values**
- **arp**
- **mbr-down**
- **mbr-map-down**
- **mbr-map-up**
- **mbr-up**
- **residual-bit-error-rate**
- **sdu**
- **thp**

All qualifying options are explained below.

---

streaming

Selects the streaming traffic class of service, which handles one-way, real-time data transmission - such as streaming video or audio. The section of the interactive traffic class can be refined with the addition of one of the following qualifying options:

- **all-values**
- **arp**
- **gbr-down**
- **gbr-up**
- **mbr-down**

- **mbr-map-down**
- **mbr-map-up**
- **mbr-up**
- **min-transfer-delay**
- **residual-bit-error-rate**
- **sdu**

All qualifying options are explained below.

---

qualif_option

Qualifying options are the QoS parameters and they include:

- **all-values** - This option will change the configuration to predefined values for *all* the relevant QoS parameters for the class. This keyword is not used if other options are to be defined. The predefined values are:

1.....Predefined QoS Parameters

QoS Parameter	Predefined Value
Traffic Class	**Background**
SDU delivery order	No
Delivery of Erroneous SDUs	No
Max Bit Rate Uplink	64 kbps
Max Bit Rate Downlink	64 kbps
Allocation/Retention Priority	3
SDU Max Size	1500 octets
SDU Error Ratio	3 (1 * 10 ^ -3)
Residual Bit Error Rate	4 (4 * 10 ^ -3)
Traffic Class	**Conversational**
SDU delivery order	No
Delivery of Erroneous SDUs	No
Max Bit Rate Uplink	16 kbps
Max Bit Rate Downlink	16 kbps
Allocation/Retention Priority	3
Guaranteed Bit Rate Uplink	16 kbps
Guaranteed Bit Rate downlink	16 kbps
SDU Max Size	1500 octets

QoS Parameter	Predefined Value
Minimum Transfer Delay	100 milliseconds
SDU Error Ratio	1 (1 * 10 ^ -2)
Residual Bit Error Rate	1 (5 * 10 ^ -2)
Traffic Class	**Interactive**
SDU delivery order	No
Delivery of Erroneous SDUs	No
Max Bit Rate Uplink	64 kbps
Max Bit Rate Downlink	64 kbps
Traffic Handling Priority	3
SDU Max Size	1500 octets
SDU Error Ratio	3 (1 * 10 ^ -3)
Residual Bit Error Rate	4 (4 * 10 ^ -3)
Traffic Class	**Streaming**
SDU delivery order	No
Delivery of Erroneous SDUs	No
Max Bit Rate Uplink	16 kbps
Max Bit Rate Downlink	16 kbps
Allocation/Retention Priority	3
Guaranteed Bit Rate Uplink	16 kbps
Guaranteed Bit Rate downlink	16 kbps
SDU Max Size	1500 octets
Minimum Transfer Delay	300 milliseconds
SDU Error Ratio	7 (1 * 10 ^ -3)
Residual Bit Error Rate	1 (5 * 10 ^ -2)

- **arp** - Sets the allocation/retention priority. Enter an integer from 1 to 3.
- **gbr-down** - Guaranteed Kbps rate for the downlink direction. Enter an integer from the range 1 to 256000.
- **gbr-up** - Guaranteed Kbps rate for the uplink direction. Enter an integer from 1 to 256000.
- **mbr-down** - Maximum Kbps rate for the downlink direction. Enter an integer from the range 1 to 256000.

- **mbr-map-down from** *from_kbps* **to** *to_kbps* - Map received HLR MBR (**from** value) to a locally configured downlink MBR value (**to** value):
  - *from_kbps* - Enter an integer from 1 to 25600.
  - *to_kbps* - Enter an integer from 1 to 25600.
- **mbr-map-up from** *from_kbps* **to** *to_kbps* - Map received HLR MBR (**from** value) to a locally configured uplink MBR value (**to** value):
  - *from_kbps* - Enter an integer from 1 to 25600.
  - *to_kbps* - Enter an integer from 1 to 25600.
- **mbr-up** - Maximum Kbps rate for the uplink direction. Enter an integer from 1 to 256000.
- **min-transfer-delay** - Minimum transfer delay in milliseconds. Enter an integer from 80 to 4000.
- **residual-bit-error-rate** -
  - Background TC residual-bit-error-rate range is from 4*10^-4 to 6*10^-8. Enter on of the following integers, where:
    - **4**: represents 4*10^-3
    - **7**: represents 10^-5
    - **9**: represents 6*10^-8
  - Conversational TC residual-bit-error-rate range is from 5*10^-2 to 10^-6. Enter one of the following integers, where:
    - **1**: represents 5*10^-2
    - **2**: represents 10^-2
    - **3**: represents 5*10^-3
    - **5**: represents 10^-3
    - **6**: represents 10^-4
    - **7**: represents 10^-5
    - **8**: represents 10^-6
  - Interactive TC residual-bit-error-rate range is from 4*10^-4 to 6*10^-8. Enter one of the following integers, where:
    - **4**: represents 4*10^-3
    - **7**: represents 10^-5
    - **9**: represents 6*10^-8
  - Streaming TC residual-bit-error-rate range is from 5*10^-2 to 10^-6. Enter one of the following integers, where:
    - **1**: represents 5*10-2
    - **2**: represents 10^-2
    - **3**: represents 5*10^-3
    - **5**: represents 10^-3
    - **6**: represents 10^-4

- **7**: represents 10^-5
- **8**: represents 10^-6

- **sdu** - Signalling data unit keyword, must include one of the following options:
  - **delivery-order**- Enter one of the two following options:
    - **no**- Without delivery order
    - **yes**- With delivery order
  - **erroneous**- Enter one of the two following options:
    - **no**- Erroneous SDUs will not be delivered
    - **no-detect**- Erroneous SDUs are not detected ('-')
    - **yes**- Erroneous SDUs will be delivered
  - **error-ratio**- The SDU error-ratio range is from 10^-3 to 10^-6. Enter an integer from 1 to 6, where:
    - **3**- Represents 10^-3
    - **4**- Represents 10^-4
    - **6**- Represents 10^-6
  - **max-size**- Defines the maximum number of octets (size) of the SDU. Enter an integer from 10 to 1502.
- **thp** - Sets the traffic handling priority. Enter an integer from 1 to 3.

Usage

This command defines the qualifying options (parameters) for each QoS traffic class defined for this APN profile.

Important: Typically this command is only used to define QoS parameters when the APN record does not exist in the subscription record.

Repeat the command as often as needed with different options to define all required QoS criteria. For example, to configure the maximum bit rate (MBR) for the downlink and uplink directions for a traffic class, this command must be used twice, specifying **mbr-down** once and **mbr-up** once.
Advantage for local mapping of MBR: some HLRs cannot be configured with high MBR values. Using the **mbr-map-up** and the **mbr-map-down** parameters allows the SGSN to be configured to treat a specific HLR value as meaning the desired high MBR value. In a case where the HLR does not support HSPA+ bit rates, but the handsets and network do, this feature allows the operator to overcome limitations on the HLR and provide HSPA+ bit rates by overwriting the provisioned HLR-QoS MBR values with SGSN-configured values. When MBR mapping is configured, if QoS is preferred as the HLR value, then the subscription QoS MBR received from the HLR is compared with the "from" value in the table. If it matches, then it is converted to the value specified by the "to" value in the table. QoS negotiation happens based on the converted value.
Advantage for QoS capping with THP and ARP: Controlling THP and ARP via Operator Policy: This functionality can differentiate home vs. roaming subscribers, and prevent visiting subscribers from receiving a high-tiered service. For example, a service provider could offer service differentiation using Ultra/Super/Standard service levels based upon QoS; this could justify charging a corporate customer more to

use the Internet APN than would be charged to a consumer. This could be accomplished by controlling the traffic handling priority (THP) over the air interface, i.e. THP 1 = Ultra, THP 2 = Super and THP 3 = Standard.

Example

Use the following command to configure the entire conversational traffic class with predefined QoS options:

```
qos class conversational all-values
```

Now change the background class ARP from 3 to 2:

```
qos class background arp 2
```

Invalidate the THP parameter, by removing all value from the parameter, for the interactive class:

```
remove qos class interactive thp
```

qos dedicated-bearer

Configures the quality of service maximum bit rate (MBR) parameters for the dedicated bearer. This command is specific to the MME.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

qos dedicated-bearer mbr max-ul *mbr-up* **max-dl** *mbr-dwn*

remove qos dedicated-bearer

remove

Removes the dedicated bearer maximum bit rate (MBR) changes from the configuration for this APN profile.

max-ul *mbr-up* **max-dl** *mbr-dl*

Defines the maximum bit rates for uplink and downlink traffic.
mbr-up is an integer from 0 through 1410065408.
mbr-dl is an integer from 0 through 1410065408.

Usage

Use this command to define the MBRs that will be enforced by the P-GW for both uplink and downlink traffic shaping.

Example

```
qos dedicated-bearer mbr max-ul 24234222 max-dl 23423423
```

qos default-bearer

Configures the quality of service parameters for the default bearer. This command is specific to the MME.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

```
qos default-bearer { arp arp_value [ preemption-capability { may | shall-not } |
vulnerability { not-preemptable | preemptable } ] | qci qci }

remove qos default-bearer { arp | qci }
```

remove

Removes the default bearer QoS configuration from this APN profile.

arp *arp_value*

Defines the address retention priority value. *arp_value* is an integer from 1 through 15.

preemption-capability { may | shall-not }

Specifies the preemption capability flag. Options are:

- **may**: Bearer may be preempted
- **shall-not**: Bearer shall not be preempted

vulnerability { not-preemptable | preemptable }

Specifies the vulnerability flag. Options are:

- **not-preemptable**: Bearer cannot be preempted.
- **preemptable**: Bearer can be preempted.

qci *qci*

Specifies the QoS Class Identifier for the default bearer profile. *qci* is an integer from 0 through 255.

Usage

Use this command to set the QoS APR and QCI parameters for the default bearer configuration.

Example

```
qos default-bearer arp 2 preemption-capability may
```

qos prefer-as-cap

Specifies operational preferences for QoS parameters, specifically QoS bit rates. This command is specific to the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
qos prefer-as-cap { both-hlr-and-local | hlr-subscription | local }

remove qos prefer-as-cap
```

Important: Command and keyword names have changed. **prefer** has become **prefer-as-cap** and **hlr** has become **hlr-subscription**. These changes will not impact configuration generated with earlier releases as the keywords are aliases for the previous names.

remove

Removes previous configuration changes and resets the default.

both-hlr-and-local

Instructs the SGSN to use, as the capping value during session establishment, the lower of either the locally configured QoS bit rate or the Home Location Register (HLR) subscription.

hlr-subscription

Instructs the SGSN to take the QoS bit rates from the HLR configuration and use the HLR rate as the capping value for session establishment.
Default.

local

Instructs the SGSN to take the QoS bit rate from the local configuration and use it for session establishment.

Usage

Use this command to instruct the SGSN to take QoS configuration as the bit rate for session establishment.

Example

The following command specifies use of the bit rate in subscription at the HLR:

```
qos prefer-as-cap hlr-subscription
```

The following command instructs the SGSN to cap the bit rate with the lower rate of the two configurations, HLR or local:

```
qos prefer-as-cap both-hlr-and-local
```

qos rate-limit direction

Configures the actions governing the subscriber traffic flow, if the flow violates or exceeds the configured or netogiated peak or committed data-rates.

This command can be entered multiple times to specify different combinations of traffic direction and class. The SGSN only performs traffic policing if **qos rate-limit direction** is configured.

Additional information on the QoS traffic policing functionality is located in the *System Administration Guide*.

Product

SGSN, S-GW

Privilege

Security Administrator, Administrator

Syntax

```
qos rate-limit direction { downlink | uplink } [ burst-size { auto-readjust [ duration
seconds ] | bytes } ] [ class { background | conversational | interactive
traffic_priority | streaming } ] [ exceed-action { drop | lower-ip-precedence | transmit
} ] [ gbr-qci [ committed-auto-readjust durarion seconds ] ] [ non-gbr-qci [ committed-
auto-readjust durarion  seconds ] ] [ violate-action { drop | lower-ip-precedence |
transmit } ] +

remove qos rate-limit direction { downlink | uplink } [ class { background |
conversational | interactive traffic_priority | streaming } ]
```

remove

Removes the qos rate-limit direction entries from the configuration.

downlink | uplink

Apply the limits and actions configured with the other keywords to the selected link:
downlink - This is the direction from the GGSN or P-GW to the MS.
uplink - This is the direction from the MS to the GGSN or the P-GW.

burst-size { auto-readjust [duration *seconds* **] | *bytes* }**

Default: See the table of class default values in the *Usage* section below.
This keyword specifies the peak burst size allowed. System measurements for this value exclude the GTP and outer packet headers. Supported options include:

- **auto-readjust**: This keyword enables dynamic burst-size calculation using negotiated peak data-rate and negotiated committed data-rate.
- **duration** *seconds*: Must be an integer from 1 to 30; default is 1. This keyword sets the number of seconds that the dynamic burst-size calculation will last. This allows the traffic to be throttled at the negotiated rates.
- *bytes*: Must be an integer from 1 to 6000000. This value specifies the static burst size for traffic policing. This option is present for backward compatibility.

Important: Use of dynamic burst size (**auto-readjust**) for traffic policing is recommended, rather than the static burst size.

class { background | conversational | interactive *traffic_priority* **| streaming }**

The **class** keyword configures the specified traffic policing actions per traffic class, or per traffic priority in the case of interactive traffic class. The following classes are supported:

- **background**: Specifies the traffic action for traffic patterns in which the data transfer is not time-critical (for example, email exchanges).
- **conversational** : Specifies the traffic policing action for traffic patterns in which there is a constant flow of packets in each direction, upstream and downstream.
- **interactive** *traffic_priority*: Specifies the traffic policing action for traffic patterns in which there is an intermittent flow of packets in each direction, upstream and downstream.

  traffic_priority is the 3GPP traffic handling priority and can be an integer 1,2 or 3.
- **streaming**: Specifies the traffic policing action for traffic patterns in which there is a constant flow of data in one direction, either upstream or downstream.

Important: This is an SGSN-specific feature. If this keyword is omitted, the same values are used for all classes.

exceed-action { drop | lower-ip-precedence | transmit }

Default: See the table of class default values in the *Usage* section below.
The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

- **drop**: Drop the packet
- **lower-ip-precedence**: Transmit the packet after lowering the ip-precedence
- **transmit**: Transmit the packet

gbr-qci [committed-auto-readjust durarion *seconds* **]**

Applies the traffic policing policy to guaranteed bitrate bearers.
committed-auto-readjust duration *seconds*: Must be an integer from 1 to 30. This keyword sets the number of seconds that the committed burst-size calculation will last. This allows the traffic to be throttled to the negotiated rates.

Important: This is an S-GW-specific feature.

non-gbr-qci [committed-auto-readjust durarion *seconds* **]**

Applies the traffic policing policy to non-guaranteed bitrate bearers.
committed-auto-readjust duration *seconds*: Must be an integer from 1 to 30. This keyword sets the number of seconds that the committed burst-size calculation will last. This allows the traffic to be throttled to the negotiated rates.

Important: This is an S-GW-specific feature.

violate-action { drop | lower-ip-precedence | transmit }

Default: See the table of class default values in the *Usage* section below.
The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **drop**: Drops the packet
- **lower-ip-precedence**: Transmits the packet after lowering the IP precedence
- **transmit**: Transmits the packet

+

This symbol indicates that the keywords can be entered multiple times within a single command.

Usage

This command configures the APN's quality of service (QoS) traffic policing. Configured actions prevent subscriber flow exceeding or violating configured peak or negotiated peak or committed data rate limits.

Important: If either **exceed action** or **violate action** is set to **lower-ip-precedence**, this command may override the configuration of the **ip qos-dscp** command in the APN profile.

Class: Background	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop
Class: Conversational	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): 16000000 Burst Size (in bytes): 65535 Exceed Action: lower-ip-precedence Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): 8640000 Burst Size (in bytes): 65535 Exceed Action: lower-ip-precedence Violate Action: drop
Class: Interactive, Traffic Handling Priority: 1	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop
Class: Interactive, Traffic Handling Priority: 2	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop
Class: Interactive, Traffic Handling Priority: 3	

Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop
Class: Streaming	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Burst Size (in bytes): 65535 Exceed Action: n/a Violate Action: drop

Example

The following command lowers the IP precedence when the committed-data-rate and the peak-data-rate are violated in uplink direction:

```
qos rate-limit direction uplink violate-action lower-ip-precedence
```

The following command drops the excess user packets when the subscriber traffic violates both the configured peak and the committed data-rate in the uplink direction. Once either the peak or the committed data-rate for that subscriber goes below the configured/negotiated limit, it transmits them.

```
qos rate-limit direction uplink exceed-action drop
```

ranap allocation-retention-priority-ie

Configures the allocation/retention priority (ARP) IE for this APN profile. This command is specific to the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ranap allocation-retention-priority-ie subscription-priority *priority* **class { { background | conversational | interactive | streaming } { not-pre-emptable | priority | queuing-not-allowed | shall-not-trigger-pre-emptable } + }**

Important: All parameters not specifically configured will be included in the configuration with default values.

[default | remove | no] ranap allocation-retention-priority-ie [subscription-priority *priority* **class { background | conversational | interactive | streaming }]**

default

Resets the configuration to the default values.

no

Disables the specified configuration

remove

Removes the specified configuration.

subscription-priority *priority*

This keyword sets the subscription priority. The lowest number has the highest priority. *priority* must be an integer from 1 to 3.

class

Configure allocation/retention priority (ARP) for specific QoS traffic classes. Include one or more of the following class options:

- **background**: background class of service
- **conversational**: conversational class of service
- **interactive**: interactive class of service
- **streaming**: streaming class of service

Default values will be included in the configuration for any class configuration not specified.

qualifying options

For each of the class options, the configuration must include one or more of the following qualifying options:

- **not-pre-emptable**

- **priority**: smallest number is the highest priority. Value must be an integer from 1 to 15
- **queuing-not-allowed**
- **shall-not-trigger-pre-emptable**

When entering more than one option, we recommend that you do it in the order in which they are listed.

+

This symbol indicates that the keywords can be entered multiple times within a single command.

Usage

Use this command to configure values for the allocation/retention priority (ARP) IE in the radio access bearer (RAB) assignment request message for RANAP that occurs during RAB setup.
This command can be used multiple times to define multiple priorities, with different combinations of **subscription-priority** and **class**.
If the HLR returns a matching value for the subscribed ARP for the desired traffic class, the SGSN includes the configured qualifying options for the ARP IE in the RANAP message.
If there is no matching configuration, the SGSN includes the following default values for the traffic class within the ARP IE:

- Default values for traffic class = background:
  priority-level = (subscribed-value * 3) + 3
  pre-emption-capability = may-trigger-pre-emption
  pre-emption-vulnerability = pre-emptable
  queuing-allowed = yes
- Default values for traffic class = conversational:
  priority-level = (subscribed-value * 3) + 2
  pre-emption-capability = may-trigger-pre-emption
  pre-emption-vulnerability = pre-emptable
  queuing-allowed = yes
- Default values for traffic class = interactive:
  priority-level = (subscribed-value * 3) + 3
  pre-emption-capability = may-trigger-pre-emption
  pre-emption-vulnerability = pre-emptable
  queuing-allowed = yes
- Default values for traffic class = streaming:
  priority-level = (subscribed-value * 3) + 1
  pre-emption-capability = may-trigger-pre-emption
  pre-emption-vulnerability = pre-emptable
  queuing-allowed = yes

Example

The following series of commands define the highest priority for conversational traffic class with priority level 1-10 (Subscribed priority 0-3), PCI of shall-not-trigger-pre-emption, PVI of not-pre-emptable with queuing-not-allowed:

```
ranap allocation-retention-priority-ie subscription-priority 0 priority
class conversational not-pre-emptable priority 1 shall-not-trigger-pre-
emptable

ranap allocation-retention-priority-ie subscription-priority 1 priority
class conversational not-pre-emptable priority 4 shall-not-trigger-pre-
emptable

ranap allocation-retention-priority-ie subscription-priority 2 priority
class conversational not-pre-emptable priority 7 shall-not-trigger-pre-
emptable

ranap allocation-retention-priority-ie subscription-priority 3 priority
class conversational not-pre-emptable priority 10 shall-not-trigger-pre-
emptable
```

restrict access-type

Configures the activation restrictions of PDP context on the basis of the access type and QoS class. This command is specific to the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
restrict access-type { { gprs | umts } [ qos-class { background | conversational |
interactive | streaming } ] }

no restrict access-type { gprs | umts } [ qos-class ]

default restrict access-type { gprs | umts }
```

no

Remove the restriction rules for PDP context activation configured in this APN profile.

default

Resets the restriction rules for PDP context activation to the default values to allow all access types and QoS class.

gprs

Configures the APN profile to restrict the PDP context activation from General Packet Radio Service (2.5G) network access.

umts

Configures the APN profile to restrict the PDP context activation from Universal Mobile Telecommunications Systems (3G) network access.

qos-class

Configures the APN profile to restrict the PDP context activation for to a specific QoS traffic class. It is optional and can be configured after selecting the network access type. Possible traffic classes options are:

- **background**: Specifies the QoS class as background service session
- **conversational**: Specifies the QoS class as conversational service session
- **interactive**: Specifies the QoS class as interactive service session
- **streaming**: Specifies the QoS class as streaming service session

Usage

Use this command to configure the restriction rules in an APN profile for activation of PDP context on the basis of the access type. It also provides the facility to restrict type of traffic QoS class.

Example

The following command configures the APN profile to restrict all traffic from a GPRS network service having a QoS class of interactive:

```
restrict access-type grps qos-class interactive
```

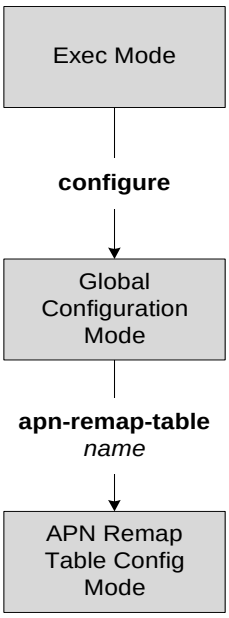
Chapter 25
APN Remap Table Configuration Mode

APN Remap Table Configuration mode provides the commands to configure parameters for multiple features related to Access Point Name (APN) handling, such as: Default APN, APN Remap, and Wildcard APN. APN remap table is a key element of the Operator Policy feature and a table is not usable (valid) until it has been associated with an operator policy (see the *Operator Policy Configuration Mode Commands* chapter.)

A maximum of 1,000 APN remap tables are supported, and each APN remap table supports a maximum of 100 APN remap entries. Multiple tables can be defined and stored but an operator policy and/or IMEI profile each only support association with a single (one) table per policy/profile configuration. The APN remap table associated with an IMEI profile will be used in IMEI override scenarios.

When this mode is accessed, the command prompt should be similar to:

```
[local]asr5000(apn-remap-table<table_id>)#
```



apn-remap

Creates an entry in the APN remap table and provides the ability override the APN requested by the UE.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

apn-remap { network-identifier *apn_net_id* **{ new-ni** *new_apn_net_id* **| operator-identifier** *apn_op_id* **new-ni** *new_apn_net_id* **{ new-oi** *new_apn_op_id* **| value-for-oi-mcc** *mcc* **| value-for-oi-mnc** *mnc* **} | value-for-ni-wc** *new_apn_net_id* **} | operator-identifier** apn_op_id **{ new-oi** *new_apn_op_id* **| value-for-oi-mcc** *mcc* **| value-for-oi-mnc** *mnc* **} }**

no apn-remap { network-identifier *apn_net_id* **| operator-identifier** *apn_op_id* **}**

no

Delete the specified APN remap entry from the APN remap table.

network-identifier *apn_net_id*

Identifies the "old" APN network identifier that is being mapped for replacement as an alphanumeric string of 1 to 62 characters, including dots (.) and dashes (-). Additionally, one wildcard character (*) can be included anywhere within the string.

new-ni *new_apn_net_id*

Identifies the new (target) network identifier to use when no wildcard character is included in the “old” APN network identifier. *new_apn_net_id* is an alphanumeric string of 1 to 62 characters, including dots (.) and dashes (-).

value-for-ni-wc *new_apn_net_id*

Identifies the information to replace the wildcard in the new APN network identifier. Use this keyword when a wildcard character is included in the “old” APN network identifier.
new_apn_net_id is an alphanumeric string of characters, including dots (.) and dashes (-). This string replaces the wildcard (*) specified in the *apn_net_id*. The two strings together must not exceed 62 characters.

operator-identifier *apn_op_id*

Identifies the “old” APN operator identifier that is being mapped for replacement. *apn_op_id* is an alphanumeric string of 1 through 18 characters including dots (.). The entry must be in the following format, where # represents a digit: `MNC###.MCC###.GPRS`.
Optionally, either one or two wildcard characters (*) can be entered. Wildcard characters can be used in place of one # or three # -- for example `MNC1*.MCC*.GPRS`.

new-oi *new_apn_op_id*

Identifies the new (target) operator identifier to use when no wildcard character is included in the "old" APN operator identifier. *new_apn_op_id* is an alphanumeric string of 1 through 18 characters including dots (.). The entry must be in the following format, where # represents a digit: MNC###.MCC###.GPRS.

value-for-oi-mcc *mcc*

Identifies the information to replace the wildcard in the new APN operator identifier when a wildcard character is included in the MCC portion of the "old" APN operator identifier, for example MNC###.MCC*.GPRS.

value-for-oi-mnc *mcc*

Identifies the information to replace the wildcard in the new APN operator identifier when a wildcard character is included in the MNC portion of the "old" APN operator identifier, for example MNC*.MCC###.GPRS.

Usage

Important: Entries in the APN remap table are only valid if the table is associated with an operator policy. The same table can then be associated with an IMEI profile as IMEI-specific remap entries are not supported.

Use this command to define table entries in the APN remap table. Each entry can remap an "old" APN network identifier (NI) or "old" APN operator identifier (OI) to a new NI or OI. Mapping can be done one-to-one with a specific APN NI/OI mapped to a specific new APN NI/OI. Mapping can also be done with wildcards in the "old" APN entry mapped to wildcard replacements to dynamically create 'new' identifiers.

Example

A one-to-one APN NI remap entry is illustrated by:

```
apn-remap network-identifier 123abc.com new-ni 333CBC.com
```

Create an entry with a wildcard so that part of an incoming APN NI will be replaced - for example, incoming "xyzabcpqr.com" becomes "xyzinternet2pqr.com".

```
apn-remap network-identifier xyz*pqr.com value-for-ni-wc internet2
```

Replace any incoming APN NI with a new APN NI.

```
apn-remap network-identifier * value-for-ni-wc newnet.com
```

A one-to-one APN OI remap entry is illustrated by:

```
apn-remap operator-identifier MNC423.MCC222.GPRS new-oi
MNC123.MCC456.GPRS
```

Replace any incoming APN OI with a new APN OI *MNC123.MCC456.GPRS*:

```
apn-remap operator-identifier MNC*.MCC*.GPRS value-for-oi-mnc 123 value-
for-oi-mcc 456
```

apn-selection-default

Enables and configures or disables the Default APN feature for use when the normal APN selection process fails.

Product

MME, SGSN

Privilege

Security Administrator, Administrator

Syntax

apn-selection-default { first-in-subscription | network-identifier *apn_net_id* **[fallback-apn network-identifier** *apn_net_id* **| fallback-to-first-in-subscription | prefer-single-subscription | reject-blank-apn | require-dns-fail-wildcard | require-subscription-apn] + }**

no apn-selection-default

no

Delete the configuration statement and disable the default APN feature.

first-in-subscription

Specifies that the first APN in the subscription record matching the PDN type is used as the default APN when normal APN selection fails and if the UE APN is absent and the defined default APN is not a match. For the SGSN, “first-in-subscription” means the first record from the list of records sent from the HLR (in the same order) with PDP type matching the requested PDP type. With this configuration, if the first record is a wildcard APN it is expected that the wildcard APN be configured. If not, the activation will be rejected.

network-identifier *apn_net_id*

Specifies the network identifier will be used as the default APN name as an alphanumeric string of 1 through 62 characters, including dots (.) and dashes (-).
Any of the following optional keywords can be used with **network-identifier** as qualifications.

fallback-apn network-identifier *apn_net_id*

SGSN only.
Specifies a dummy APN to be used when the default APN is not present in the subscription so that the activation does not fail. With this keyword configured, the context is activated with a dummy APN and the GGSN displays a static page for this APN, instructing the subscriber to subscribe for appropriate services.
apn_net_id: Enter an alphanumeric string of 1 through 62 characters, including dots (.) and dashes (-).

fallback-to-first-in-subscription

Uses the APN from the first subscription record when configured default APN is not available.

prefer-single-subscription

Uses the APN from the subscription record if it is the only record available and normal APN selection fails.

reject-blank-apn

Disables use of the default APN if a blank APN is received.

require-dns-fail-wildcard

Enables the default APN to be used if the DNS query fails with the selected APN.

require-subscription-apn network-identifier *apn_net_id*

If defined, this APN name must also be included in the subscription data for the Default APN feature to function. *apn_net_id* is an alphanumeric string of 1 through 62 characters, including dots (.) and dashes (-).

Usage

Important: The Default APN feature will only work if it is configured in an APN remap table entry and the table is associated to an IMEI profile.

The default APN feature will be used in error situations when the SGSN cannot select a valid APN via the normal APN selection process. Within an operator policy, a default APN can be configured for the SGSN to:

- override a requested APN when the HLR does not have the requested APN in the subscription profile.
- provide a viable APN if APN selection fails because there was no "requested APN" and wildcard subscription was not an option.

The default APN feature can also be used in the event of a DNS query failure with the selected APN, if:

- the **wildcard-apn** command is configured,
- a wildcard subscription is present,
- the **require-dns-fail-wildcard** keyword is included with the **apn-selection-default** command then the configured default APN will be used when the DNS query is retried.

In all of the instances outlined above, the SGSN can provide the default APN as an alternate behavior to ensure that PDP context activation is successful.

Example

The following command enables default APN feature for APN *HomeNet1*:

```
apn-selection-default network-identifier HomeNet1
```

The following command enables use of a default APN if the DNS query fails:

```
apn-selection-default network-identifier HomeNet1 require-dns-fail-
wildcard
```

blank-apn

Enables the Blank APN feature and defines the APN that will be used when no APN is requested. This command is specific to SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

blank-apn network-identifier *apn_net_id*

no blank-apn

no

Removes the APN NI from the APN Remap Table configuration and disables the Default APN feature.

network-identifier *apn_net_id*

Identifies the APN network identifier that will be used when no APN is requested. *apn_net_id* is an alphanumeric string of 1 through 62 characters, including dots (.) and dashes (-).

Usage

Use this command to enable the Blank APN feature.

Example

The following command creates an entry that supplies the *starnet.com* as the APN network identifier whenever a request does not include an APN:

```
blank-apn network-identifier starnet.com
```

cc

This command defines APN remapping behavior so that remapping occurs based on the charging characteristics value.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

cc behavior *bit_value* **profile** *index_bit* **apn-remap network-identifier** *apn_net_id* **new-ni** *new_apn_net_id*

no cc behavior *bit_value* **profile** *index_bit* **apn-remap network-identifier** *apn_net_id*

no

Disables the configured remapping behavior.

behavior*bit_value*

Specify the bit value for the behavior bit for the charging characteristic.
bit_value must be a hex value from 0x0 to 0xFFF.

profile *index_bit*

Specifies the charging characteristic profile index for this apn remap entry.
index_bit must be an integer value from 1 through 15.
Some of the index values are predefined according to 3GPP standard:

- **1** for hot billing
- **2** for flat billing
- **4** for prepaid billing
- **8** for normal billing

apn-remap network-identifier *apn_net_id*

Identifies the 'old' APN network identifier that is being mapped for replacement.
apn_net_id : Enter a string of 1 to 62 alphanumeric characters, including dots (.) and dashes (-) .
Additionally, one wildcard character (*) can be included anywhere within the string.

new-ni *new_apn_net_id*

Identifies the 'new' APN network identifier that is being mapped to.
new_apn_net_id : Enter a string of 1 to 62 alphanumeric characters, including dots (.) and dashes (-) .

Usage

Use this command to enable APN remapping only when the charging characteristic value in the subscription record associated with the requested APN matches the value configured for the **new-ni** .

The new APN NI must be part of the subscription data so that the charging characteristic associated with the new APN NI will be used for activating the context and if there isn't one associated then the general charging characteristic will be used.

Example

The following command associates a new APN NI 'locals1' with a set of charging characteristics:

```
cc behavior 0xF profile 4 apn-remap network-identifier homer1 new-ni
locals1
```

description

Defines a string that describes this APN remap table.

Product

MME, SGSN

Privilege

Security Administrator, Administrator

Syntax

description *description*

no description

no

Removes the description configuration from this APN Remap Table configuration.

description

Specifies descriptive text to be associated with the APN remap table as an alphanumeric string of 1 through 100 characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotation marks (“).

Usage

Define information that identifies this particularly APN remap table.

Example

```
description “APN_remap1 replaces all MNC1## Ids.”
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

wildcard-apn

Enables or disables the Wildcard APN feature and define the default APN to be used whenever a wildcard APN is included in the subscriber record.

Product

MME, SGSN

Privilege

Security Administrator, Administrator

Syntax

wildcard-apn pdp-type { dual-ipv4v6 | ipv4 | ipv6 | ppp } network-identifier*apn_net_id*

no wildcard-apn pdp-type { dual-ipv4v6 | ipv4 | ipv6 | ppp }

no

Disables the wildcard-apn definition from the configuration.

pdp-type { dual-ipv4v6 | ipv4 | ipv6 | ppp } network-identifier *apn_net_id*

Specifies the PDP type.

- **dual-ipv4v6**- for a dual PDP context association with one IPv4 address and one IPv6 address/prefix (SGSN only)
- **ipv4** - for an IPv4 context
- **ipv6** - for an IPv6 context
- **ppp** - for a PPP context

network-identifier *apn_net_id* must be one of the APN network identifiers specified via the **apn** command in the Operator Policy Configuration mode. The identifier must be expressed as an alphanumeric string of 1 through 62 characters, including dots (.) and dashes (-), to define the network identifier.

Usage

This command is used to define a wildcard APN with the type of PDP context and the APN's network ID. This wildcard APN would be used when an APN is not identified.
The command should be repeated per PDP type, as needed, to enable wildcard APN for two or more of the PDP types.
The wildcard APN configured with the dual PDP IPv4v6 context will be used under in the following scenarios:

- the UE requested a PDP type of IPv4v6
- the UE did not request any specific APN
- the subscription includes wildcard APN with PDP type as IPv4v6

Important: Wildcard APN feature configuration is only valid if the APN remap table is associated with at least one operator policy. The same table can then be associated with an IMEI profile as IMEI-specific Wildcard APN is not supported.

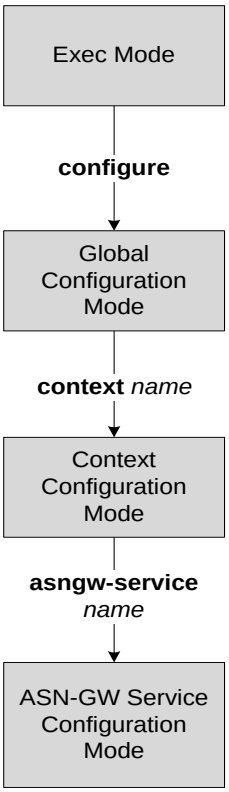
Example

Use this command to enable an APN wildcard for PDP type IPv4:

```
wildcard-apn pdp-type ipv4 network-identifier homer1
```

Chapter 26
ASN Gateway Service Configuration Mode Commands

Use the ASN GW Service Configuration Mode to create and manage ASN Gateway services within the current context.



active-relay

Use this command to enable the active relay of R4 and R6 messages in ASN GW, and to configure the timeout duration in seconds for the R4 or R6 messages (for example, Data Path messages).

Product

ASN GW

Privilege

Administrator

Syntax

active-relay timeout < *duration*>

[default] active-relay timeout

default

Sets the total timeout duration to 15 seconds to actively relayed R4 or R6 messages.

duration

Default: 15
Specifies the maximum allowable timeout duration for the ASN GW service to actively relay the R4 or R6 messages.
duration is measured in seconds. Configure as an integer from 5 through 65535.

Usage

Use this command to enable the active relay of R4 and R6 messages and also to configure the maximum timeout duration for the actively relayed R4 or R6 messages by ASN GW.
By default, the system is pre-configured for passive relay functionality for R4 and R6 messages.

Example

The following command configures the timeout duration of *20* seconds for actively relayed R4 or R6 messages:

active-relay timeout *20*

authentication

Use this command to configure the authentication type and parameters used for subscribers in this service.

Product

ASN GW

Privilege

Administrator

Syntax

```
authentication { single-eap |  none }

default authentication
```

default

Disables the authentication requirement for the ASN GW service.

single-eap

This keyword enables single Extensible Authentication Protocol (EAP) authentication for specific ASN GW service subscribers. Possible single-EAP authentication options are User-only, Device-only, or Device-User.

none

This is the default setting for authentication. Enter this keyword to disable all authentication types for a specific ASN GW service.

Usage

Use this command to configure authentication requirements for the ASN GW service.

Example

The following command sets the user authentication for ASN GW service with single EAP:

```
authentication single-eap
```

bind

Use this command to bind the ASN GW service to a logical IP interface and to configure the maximum number of subscribers supported within an ASN GW service.

Product

ASN GW

Privilege

Administrator

Syntax

bind address *ip_address* **[max-subscribers** *max_subs* **]**

no bind

no

Removes the binding of the service to a specified interface.

ip_address

Specifies the IP address of the interface to which the service is to be bound. Express *ip_address* in IPv4 dotted decimal or IPv6 colon-separated notation.

max-subscribers *max_subs*

Configures the maximum number of subscribers allowed to connect with this ASN Gateway within a specific ASN GW service.
max_subs must be an integer from 1 and 1500000.

Usage

Use this command to associate the service with a specific logical IP address and provide the identity of the ASN Gateway. The identity is either the domain name of the ASN GW service or the IP address. This command also configures the maximum number of subscribers with this service.

Example

The following command binds the ASN GW service to a logical interface with an IP address of *1.2.3.4* with a limit of *250000* subscribers:

```
bind address 1.2.3.4 max-subscribers 250000
```

bs-monitor

Use this command to enable or disable the ASN base station monitoring and related parameters in a WiMAX ASN.

Product

ASN GW

Privilege

Administrator

Syntax

bs-monitor [interval *duration* **| num-retry** *retries* **| timeout** *idle_time* **]**

[default | no] bs-monitor

default

Disables the configured BS monitoring parameters.

no

Removes the configured BS monitoring feature and parameters.

interval *duration*

Default: 60
Configures the interval duration in seconds between two ICMP ping messages sent to the ASN BS for BS monitoring.
duration specifies the amount of time in seconds between two ICMP ping messages sent to monitor an ASN BS. Specify an integer from 1 through 36000.

num-retry *retries*

Default: 5
Configures the number of retries before marking a specific ASN BS as unreachable.
retries specifies the number of times to send ICMP ping messages to an ASN BS before the ASN BS is declared unreachable. Enter an integer from 0 through 100.

timeout *idle_time*

Default: 3
Configures the timeout duration to wait for a response from ASN BS of ICMP ping message before retransmitting the ICMP ping packets.
idle_time must be an integer value in the range of 1 through 10.

Usage

Use this command to enable or disable base station monitoring and to configure the ASN BS monitoring parameters in a WiMAX ASN.

Important: Base Station Monitoring is a license-enabled feature.

Example

The following command configures the timeout duration of *5* seconds before sending an ICMP ping message if the ASN BS does not respond:

bs-monitor timeout *6*

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

gre

This command configures the GRE tunnel parameters for ASN GW gateway functionality within a specific ASN GW service.

Product

ASN GW

Privilege

Administrator

Syntax

gre mtu *mtu_size*

default gre mtu

default

Sets the MTU size for the GRE tunnel to the default value of 1500 bytes in a WiMAX network.

mtu *mtu_size*

Default: 1500 bytes
Configures the maximum transmission unit size in bytes for the GRE tunnel within a specific ASN GW service.
mtu_size must be an integer between 36 and 2000.

Usage

Use this command to support tunnel reassembly optimization with the MTU size for a GRE tunnel in a WiMAX network.

Example

The following command configures the maximum transmission unit (MTU) size to *1700* bytes for a GRE tunnel:

```
default gre mtu 1700
```

handover

This command specifies the handover-related parameters between BS, ASN GW, and MS.

Product

ASN GW

Privilege

Administrator

Syntax

handover { anchor { dp-pre-reg-termination timeout *duration*| **dp-termination timeout** *duration* **} | max-dp-pre-registrations** *reg_num* **| non-anchor { dp-pre-reg-termination timeout** *duration* **| dp-termination timeout** *duration* **} }**

default handover { anchor { dp-pre-reg-termination timeout | dp-termination timeout } | max-dp-pre-registrations | non-anchor { dp-pre-reg-termination timeout | dp-termination timeout } }

default

Sets the default values for configured handover parameters.

anchor

Configures datapath pre-registration and/or termination parameters for an anchor gateway handover.

dp-pre-reg-termination timeout *duration*

Default: 5
Configures the maximum duration in seconds that a single MS can keep the pre-registration datapath with the previous BS after a completed handover to another BS.
duration is measured in seconds. Configure as any integer from 0 through 65535.

dp-termination timeout *duration*

Default: 0
Configures the maximum duration in seconds for which the datapath with the previous BS is maintained after a completed handover to another BS. The system maintains the old datapath for the specified period after the new datapath setup is completed, and then terminates it.
duration is measured in seconds. Configured as any integer from 0 through 65535.

max-dp-pre-registrations *reg_num*

Default: 1
Configures the maximum number of pre-registrations from multiple BSs that a single MS can keep at a time.
reg_num is the number of pre-registrations. Configure as any integer from 0 through 5.

non-anchor

Configures datapath pre-registration and/or termination parameters for a non-anchor gateway handover.

Usage

Use this command to configure the handover-related parameters between MS, BS, and ASN GW.
By default, the system is configured to terminate the previous sessions immediately. The number of pre-registrations from multiple BSs is set to 0 for an MS.

Example

The following command configures the maximum duration as *20* seconds. This is the amount of time for which the datapath with the previous BS is maintained after a completed handover to another BS:

```
dp-pre-reg-termination timeout 20
```

header-compression-rohc

Use this command to configure (Robust Header Compression (ROHC) support and ROHC parameters in an ASNGW service. Header compression is applied to ASNGW service flows when the ROHC is enabled on the ASNGW, and MS and AAA authorize ROHC for the ASNGW call. If ROHC is supported on the service, it is indicated in the MS attachment messages. ROHC parameter values are negotiated over R6. Unidirectional and bi-directional ROHC service flow are supported.

Product

ASN GW

Privilege

Administrator

Syntax

header-compression rohc { [default] | cid-mode-large max-cid < *max-cid* > **| cid-mode-small** < *max-cid* > | **mrru** < *integer* > } **profile-id { rtp- ip | esp-ip | rtp-udp | udp-ip | uncompressed-ip}**

header-compression rohc

Sets the default values for configured ROHC parameters.

default

Sets the default values for configured ROHC parameters.

cid-mode-large max-cid

ROHC large context identifier range mode: an integer from 0 to 31.

cid-mode-small max-cid

ROHC small context identifier range mode: an integer from 0 to 15.

mrru

Maximum Reconstructed Reception Unit: The maximum possible size of a packet reassembled from ROHC segments: an integer from 0 to 65535.

profile id

The ROHC configuration is controlled by a set of attributes which are assocated with an ROHC profile. A system may have multiple profiles..

Usage

Data packets that are transferred over a wireless link are dependent on each other and share common parameters, such a equal source and destination addresses. They can usually be grouped together logically, for example, data packets that constitute an audio stream and data packets that make up the accompanying video stream. Therefore, you can use a stream-oriented approach in ROHC to compress packet headers. Each stream or flow is identified by its parameters that are common to all packets in a particular stream. The compressor and decompresor maintain a context for each stream, which is identified by the same context

identifier (CID) on both sides. A context, being a set of data, contains, for example, the statis and dynamic header fields that define a stream.

Example

The following command configures a small context ROHC CID.

```
header-compression rohc cid-mode small max 15 profile-id udp-id
```

idle-mode

Use this command to configure the time in seconds that an ASN GW service waits to place a session in idle mode or reactivates an idle session after the specified time for exit timeout. This occurs if there is no activity for the amount of time you specified.

Product

ASN GW

Privilege

Administrator

Syntax

idle-mode { entry-timeout *duration* **| exit-timeout** *duration* **| timeout** *duration* **}**

default idle-mode { entry-timeout | exit-timeout | timeout }

default

Resets the idle mode durations to their respective default values.

no

Disables/removes the configured idle mode entry and/or exit timeout duration for a session.

entry-timeout *duration*

Default: 60
Specifies the maximum duration in seconds allowed for idle mode entry for a session.
duration is measured in seconds. Configure as an integer from 1 through 100000.

exit-timeout *duration*

Default: 60
Specifies the maximum duration in seconds allowed for session to reenter active mode after idle mode exit.
duration is measured in seconds. Configure as an integer from 1 through 100000.

timeout *duration*

Default: 4069
Specifies the maximum time (in seconds) allowed for a session to remain in idle mode. *duration* is an integer from 128 to 65535.

Usage

Use this command to configure the ASN GW service to send a session for idle mode or active mode after specified duration of time.

Example

The following command configures the idle mode entry timeout value to *50* seconds:

```
idle-mode entry-timeout 50
```

local-data-tunnel

Use this command to specify the tunnel endpoint on the ASNGW side to receive the uplink data packets over the R6 interface. This address is different from the R6 control address.

Product

ASN GW

Privilege

Administrator

Syntax

local-data-tunnel address < *address* >

default

Default is no tunnel endpoint is configured and the control address is used as the uplink tunnel endpoint.

no

Disables/removes the configured tunnel endpoint.

address *address*

Specifies the tunnel endpoint that will receive uplink data packets over the R6 interface.

Example

The following command specifies the tunnel endpoint on the ASNGW side that will receive uplink data packets over the R6 interface.

```
local-data-tunnel address 102.168.1.5
```

max-retransmission

Use this command to specify the number of times the system can attempt retransmission of R6 control packets to communicate with an unresponsive BS.

Product

ASN GW

Privilege

Administrator

Syntax

max-retransmission *retry*

default max-retransmission

default

Sets the maximum number of retransmission counters to 3 for R6 control packets within a specific ASN GW service.

retry

Default: 3
Configures the maximum number of retransmission of R6 control packets to BS before marking it as failed. *retry* must be an integer between 1 and 10.

Usage

Use this command to configure number of retransmission of R6 control packets to BS before marking it as failed.

Example

The following command configures the system to attempt sending R6 control packets to the BS *2* times:

```
max-retransmission 2
```

mobile-access-gateway

Use this command to associate MAG context and/or MAG service for an ASNGW service. This is available only when PMIPv6 is supported and the license is enabled. Default: no

Product

ASN GW

Privilege

Administrator

Syntax

mobile-access-gateway context < *context_name* >**[mag-service**< *service-name* > **]**

no mobile-access-gateway context

Usage

MAG service is responsible for PMIPv6 signaling. MAG service establishes and maintains a bi-directional tunnel for the subscriber traffic with LMA.
Use the **no mobile-access-gateway context** to delete a previously configured context.

Example

The following command instructs the ASN GW service to use the context named mag-service for MAG functionality:

mobile-access-gateway context *context-name***mag-service** *service-name*

mobile-ip

This command configures Mobile IP support with FA service(s) for specific ASN GW service and specifies the context in which the FA service is configured. Default: no

Product

ASN GW

Privilege

Administrator

Syntax

mobile-ip foreign-agent context *context_name*

no mobile-ip foreign-agent context

foreign-agent context *context_name*

Default: No FA context specified.
Specifies the name of the previously configured context that facilitates the FA service(s).
context_name must be between 1 and 79 alpha or numeric characters and is case sensitive.

Usage

You can configure FA services on the system in either the same or different contexts from those facilitating ASN GW services. When they are configured in separate contexts, this command, configured within an ASN GW service, instructs the ASN GW service to route traffic to the context facilitating the FA service.
Use the **no mobile-ip foreign-agent context** to delete a previously configured destination context.

Example

The following command instructs the ASN GW service to use the context named FA-destination for FA functionality:

mobile-ip foreign-agent context *fa-destination*

peer-asngw

Use this command to configure the addresses of trusted non-anchor ASN GWs or ASN PC/LR peers for which a specific ASN GW service can allow R4 control and data path registration.

Product

ASN GW

Privilege

Administrator

Syntax

[no] peer-asngw address < *ip_address*> **[id** < *6-byte MAC address* > | **mode** {*legacy* | *non-legacy* } | < *simple-ip re-anchoring* >]

no

Removes the configured non-anchor ASN GW or non-anchor ASN PC/LR peers from a specific ASN GW service's trusted peer list.

peer-asngw address

Specifies the IP address of the non-anchor ASN GW or non-anchor ASN PC/LR peers. The IP address is added as a trusted peer with the ASN GW service.
ip_address is the IP address of the non-anchor ASN GW or non-anchor ASN PC/LR peers expressed in IPv4 dotted decimal or IPv6 colon separated notation.
6-byte MAC address is the 6-byte identifier on the ASNGW service.

Usage

Use this command to create trusted non-anchor ASN GW or non-anchor ASN PC/LR peers with a specific ASN GW service to establish R4 control and data path registration. The ASN GW supports the 6-byte ASNGW ID in the souce ID TLV and destination ID TLV of all the messages. The 6-byte anchor gateway ID and authenticator ID are also supported.
On receipt of an R4 control or data path registration request message, the ASN GW service checks whether a non-anchor DPF/Authenticator ASN GW/ASN PC-LR address received in a request message, is in the trusted peer list configured with this command. If the Anchor DPF/Authenticator ASN GW/ASN PC-LR address is not configured in the non-anchor ASN GW or non-anchor ASN PC/LR peers' list, the ASN GW service sends a response for a request message with Failure Indication TLV and unspecified error code.
You can configure a maximum of 32 ASN GWs or ASN PC/LRs with this command.

Example

The following command adds the ASN GW with an IP address as a trusted peer within an ASN GW service, and a 6-byte ID for the peer ASN GW.

peer-asngw address *1.2.3.4* **id** *00-05-47-00-37-44*

policy

This command configures the policies for ASN Gateway behavior within a specific ASN GW service.

Product

ASN GW

Privilege

Administrator

Syntax

```
policy { asngw-initiated-reauth | ms-unexpected-network-reentry | msid-dhcp-chaddr-mismatch | | non-anchor-mode | overload } { allow | disallow }

default policy { ms-unexpected-network-reentry | msid-dhcp-chaddr-mismatch | non-anchor-mode }
```

default

Resets the policy parameters to their respective default values.

asngw-initiated-reauth

Defualt: allow
Configures ASNGW-initiated reauthentication parameters.

ms-unexpected-network-reentry

Default: allow
Configures the ASN Gateway to allow or disallow an MS re-entry from the same or a new BS, when an active call already exists for the same MS on the ASN Gateway.
This policy performs in the following manner:

- If the pre-attachment request of the new call comes from a different BS, re-entry is accepted regardless of the call state.
- If the pre-attachment request of the new call comes from the same BS, re-entry is accepted if the original call is in any state past the pre-attachment phase.
- Original call is dropped in favor of new call.

msid-dhcp-chaddr-mismatch

Default: disallow
Valid only for the primary host. Configures the ASN Gateway to allow or disallow an MS to connect if the MSID and DHCP address information is mismatched.

non-anchor-mode

Default: allow
Configures the ASN Gateway to allow or disallow the creation of non-anchor sessions based on the DP Registration Request from any base station.
When non-anchor mode is not allowed and a DP Registration Request is received, if there is no matching session for the MSID, the request is rejected and a DP Registration Response is sent with an error code: "**Admin Prohibited**".

overload

Default: allow

Designates the rejection of ASNGW services in case of session overload.

allow

Sets the policies to allow the MS matching with specified policy for ASN Gateway.

disallow

Sets the policies to deny or disallow the MS matching the specified policy for ASN Gateway.

Usage

Use this command to configure the policies of the ASN Gateway to handle the MS connection within a specific ASN GW service.

Example

The following command enforces the policy to allow an MS re-entry from a new BS, when an active call exists for the same MS on the ASN Gateway via another BS.:

```
policy ms-unexpected-network-reentry allow
```

policy asngw-initiated-reauth

This command configures the policies for how the ASN Gateway initiates reauthorization triggers from an ASN GW service.

Product

ASN GW

Privilege

Administrator

Syntax

policy asngw-initiated-reauth { allow | disallow | max-cmac-key-count *max_count*| **pmk-grace-time** *grace_time* **}**

default policy asngw-initiated-reauth [max-cmac-key-count | pmk-grace-time]

default

Resets the policy to disallow ASN GW-initiated re-authorization and sets the default values for CMAC key count and PMK grace time within a specific ASN GW service.

max-cmac-key-count *max_count*

Default: 100
Configures the ASN Gateway to trigger the reauthorization on the basis of Cipher-based Message Authentication Code (CMAC) key counter. Once the CMAC counter crosses the configured value, the system initiates the reauthorization trigger.
max_count is the CMAC key counter and is an integer from 2 through 32768.

pmk-grace-time *grace_time*

Default: 60
Configures the ASN Gateway to trigger the reauthorization on the basis of the Pair-wise Master Key (PMK) key grace period. Once the configured PMK grace period is exhausted, the system initiates the reauthorization trigger.
grace_time is the grace period in seconds to wait for the Pair-wise Master Key (PMK) and is an integer from 10 through 65335.

allow

Default: disabled
Configures the ASN Gateway to trigger re-authentication based on two locally configured parameters: **pmk-grace-time** and **cmac-key-count**.

disallow

Default: enabled
Configures the ASN Gateway not trigger the re-authentication based on two locally configured parameters: **pmk-grace-time** and **cmac-key-count**.

Usage

Use this command to enable the ASN GW to initiate the reauthorization trigger on the basis of the configured policy.

Example

The following command enforces the reauthorization policy from the ASN GW:

```
policy asngw-initiated-reauth allow
```

policy overload

Configures the traffic overload policy that controls congestion in this service.

Product

ASN GW

Privilege

Administrator

Syntax

```
policy overload { drop | reject }

default policy overload
```

default

Sets the traffic overload policy action to reject in this service.

drop

Default: disabled
Specifies that the system is to drop incoming packets containing new session requests.

reject

Default: enabled
Specifies that the system processes new session request messages and responds with a reject message.

Usage

You can configure congestion policies at the service-level. When congestion control functionality is enabled at the service level, these policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

Example

The following command configures an overload policy of reject for this ASN GW service:

```
policy overload reject
```

ran-peer-map

Use this command to configure a mapping between the BSID and IPv4 address of known base station peers; identifies a base station peer map for this service.

Product

ASN GW

Privilege

Administrator

Syntax

ran-peer-map *name* **ran-peer id**< *mac-addr* >**address**< *ip-addr* >**[mode {non-legacy | legacy}]**

no ran-peer-map

name

Specifies the name of the RAN Peer Map. Specify a *name* from 1 to 31 alpha and/or numeric characters. The name must be an existing peer map. Configure RAN Peer Maps in the Global Configuration Mode.

ran-peer id

Creates a mapping for id to ip address.

address

Specifies the IPv4 address of the base station which is added as a peer for the given service.

mode {non-legacy | legacy}]

Default: non-legacy

Usage

Use this command to configure a base station peer map that this service will use to map MAC addresses received in R6 protocol messages to IPv4 addresses.

Example

The following command configures the service to refer to a peer map named *ran12* when reconciling a base station MAC address to an IP address:

ran-peer-map *ran12*

retransmission-timeout

Use this command to configure the non-response time before the system re-attempts to send R6 control packets to the BS.

Product

ASN GW

Privilege

Administrator

Syntax

retransmission-timeout *duration*

[no | default] retransmission-timeout

default

Sets the timeout duration to 3 seconds before R6 control packets are retransmitted.

no

Disables or removes the configured timeout duration for the retransmission of R6 control packets.

duration

Default: 3
Specifies the the number of seconds for the ASN GW service to wait for a response from the BS before it (a) attempts to communicate with the BS again (if the system is configured to retry the BS), or (b) marks the BS as unreachable.
duration is measured in seconds and can be configured to any integer value between 1 and 1,000.

Usage

Use this command in conjunction with the **max-retransmission** command to configure the ASN GW services behavior when it does not receive a response from a particular BS.
Use the **no retransmission-timeout** command to delete a previously configured timeout value. If after deleting the lifetime setting you desire to return the lifetime parameter to its default setting, use the **default retransmission-timeout** command.
The chassis is shipped with the retransmission timeout set to 3 seconds.

Example

The following example configures a retransmission timeout value of 5 seconds:

```
retransmission-timeout 5
```

The following command deletes a previously configured retransmission-timeout setting:

```
no retransmission-timeout
```

secondary-ip-hosts

Use this command to enable or disable multiple host support behind WiMAX customer premises equipment (CPE).
Default: disabled

Product

ASN GW

Privilege

Administrator

Syntax

secondary-ip-hosts *max_hosts*

default multiple-ip-hosts

default

Sets the multiple host configuration in an ASN GW service to disabled (default mode).

max_hosts

Default: 0 (disabled)
Specifies the maximum number of hosts allowed to connect through one primary node connection behind a WiMAX CPE.
max_hosts must be an integer from 0 through 4, where 0, the default value, disables this feature.

Usage

Use this command to enable or disable multi-IP host support in an ASN GW service behind one WiMAX CPE through a primary airlink. If enabled, this command supports up to four hosts as an auxiliary connection. Accounting and UDR generation for such connections are based on the primary connection with the WiMAX CPE. To apply this facility to a subscriber, configure the **ip address secondary-pool** command in the **Subscriber Configuration** mode.

Example

The following command enables multiple host support and instructs the ASN GW service to allow *3* IP hosts as auxiliary connections behind one CPE:

```
secondary-ip-hosts 3
```

The following command disable the multiple host support and instructs the ASN GW service not to allow auxiliary connections behind one CPE:

```
default secondary-ip-host
```

secondary-ip-hosts

Use this command to enable or disable multiple host support behind WiMAX customer premises equipment (CPE).
Default: disabled

Product

ASN GW

Privilege

Administrator

Syntax

secondary-ip-hosts *max_hosts*

default multiple-ip-hosts

default

Sets the multiple host configuration in an ASN GW service to disabled (default mode).

max_hosts

Default: 0 (disabled)
Specifies the maximum number of hosts allowed to connect through one primary node connection behind a WiMAX CPE.
max_hosts must be an integer from 0 through 4, where 0, the default value, disables this feature.

Usage

Use this command to enable or disable multi-IP host support in an ASN GW service behind one WiMAX CPE through a primary airlink. If enabled, this command supports up to four hosts as an auxiliary connection. Accounting and UDR generation for such connections are based on the primary connection with the WiMAX CPE. To apply this facility to a subscriber, configure the **ip address secondary-pool** command in the **Subscriber Configuration** mode.

Example

The following command enables multiple host support and instructs the ASN GW service to allow *3* IP hosts as auxiliary connections behind one CPE:

```
secondary-ip-hosts 3
```

The following command disable the multiple host support and instructs the ASN GW service not to allow auxiliary connections behind one CPE:

```
default secondary-ip-host
```

service-flow create-before-ip-alloc

This command specifies whether service flows should be created before the IP allocation is completed. If this command is not configured, during the INE process, only an Initial Service Flow (ISF) is created with a wildcard classifier. The remaining service flow is created after the IP allocation.

Product

ASN GW

Privilege

Administrator

Syntax

```
[ no | default ]service-flow create-before-ip-alloc
```

default

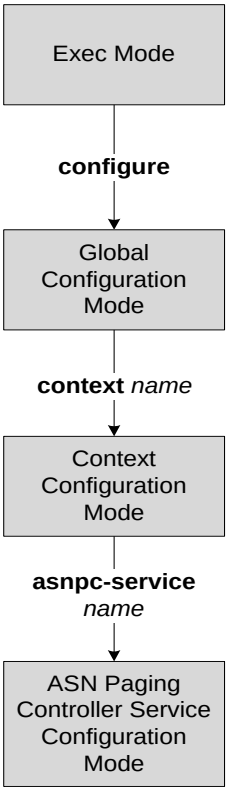
The default is *disabled*.

Usage

There are two types of service flows: 1) pre-provisioned service flows are created during INE and created, modified, or deleted based on some external trigger from the PCRF/AAA; 2) dynamic service flow creation is on an on-demand basis and because of some external trigger from the PCFR/AAA. Path modification is requested to changes in the state of the service flow, for example, from admit to active or from active to admit.

Chapter 27
ASN Paging Controller Configuration Mode Commands

Use the ASN Paging Controller Configuration Mode to create and manage Access Service netowrk (ASN) paging and location register services for WiMAX subscribers within a context.



asnpc-id

Configures the identifier for an ASN paging controller for the subscribers in this service.

Product

ASN PC-LR

Privilege

Administrator

Syntax

asnpc-id *mac_address*

default asnpc-id

default

Sets the ASN paging controller identifier as the IP address of the system running the ASN paging controller and location registry service.

mac_address

Specifies the MAC address of the system running the ASN paging controller and location registry service. *mac_address* is the MAC address of the paging controller in standard (IEEE 802) format – six groups of two hexadecimal digits separated by hyphens (-) or colons (:).

Usage

Use this command to configure the MAC address of the paging controller for the ASN paging controller service.

Example

The following command sets the MAC address of paging controller to *01:23:45:67:89:ab* in colon (:) separated format:

```
asnpc-id 01:23:45:67:89:ab
```

bind

Binds the ASN paging controller service to a logical IP interface and configures the maximum number of subscribers allowed within a service.

Product

ASN PC-LR

Privilege

Administrator

Syntax

bind address *ip_address* **[max-subscribers** *max_subs* **]**

no bind

no

Removes the binding of the service to a specified interface.

ip_address

Specifies the IP address of the interface to which the service is to be bound in IPv4 dotted-decimal or IPv6 colon-separated notation.

max-subscribers *max_subs*

is an integer from 0 through 3000000.

Usage

Use this command to associate the service with a specific logical IP address and to provide the identity of the ASN paging controller as either the domain name of the ASN paging controller service or the IP address. This command also configures the maximum number of subscribers allowed with this service.

Example

The following command binds the ASN paging controller service to a logical interface with an IP address of *10.2.3.4* and a limit of *250000* subscribers:

```
bind address 10.2.3.4 max-subscribers 250000
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

max-retransmission

Configures the maximum number of times the system attempts retransmission of R6 control packets to communicate with an unresponsive BS.

Product

ASN PC-LR

Privilege

Administrator

Syntax

max-retransmission *retry*

default max-retransmission

default

Sets the maximum number of retransmission counter to 3 for R6 control packets within a specific ASN paging controller service.

retry

Configures the maximum number of retransmission attempts of R6 control packets to the BS before marking it as unresponsive as an integer from 1 through 10. Default: 3

Usage

Use this command to configure the number of retransmission attempts of R6 control packets to the BS before marking it as unresponsive.

Example

The following command configures the system to attempt *2* tries to send R6 control packets to BS:

```
max-retransmission 2
```

paging-announce

Configures the number of seconds to wait before sending a paging announcement messages to the MS.

Product

ASN PC-LR

Privilege

Administrator

Syntax

paging-announce timeout *duration*

default paging-announce timeout

default

Sets the paging announcement timeout to 10 seconds.

duration

Specifies the maximum duration in seconds to wait for sending a paging announce to the MS as an integer from 1 through 1000. Default: 10

Usage

Use this command to configure the number of seconds for the ASN paging controller services to wait before sending a paging announcement if there is no data communication.

Example

The following command configures the paging announce timeout value of *500* seconds:

```
paging-announce timeout 500
```

paging-group

Creates or removes the Paging-Group Identifier within a specific ASN paging controller service.

Product

ASN PC-LR

Privilege

Administrator

Syntax

paging-group id *paging_group_id* **paging node id**< *mac-addr* >**addr**< *ip-addr* >**[mode {non-legacy | legacy}][-noconfirm]**

no paging-group id *paging_group_id*

no

Disables or removes the paging group identifier from a specific ASN paging controller service.

id *paging_group_id*

Configures the paging group identifier and other parameters within a specific ASN paging controller service. This is a logical network identifier for the serving BS or other network entity that retains MS service and operational information or administers paging activity for the MS while it is in idle mode
*paging_group_id*is an integer from 1 through 65535.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

WARNING: If you use this keyword option with **no paging-group id** *paging_group_id* command, the **paging group id** *paging_group_id* is deleted and disabled with all active or inactive configurations in a paging group. There are no prompts, warning, or confirmations.

Usage

Use this command to enter, enable, or disable the Paging Group Identifier Configuration mode functionality within a specific ASN paging controller service.

Important: Configure a maximum of 32 paging groups within a service.

Example

The following command configures the paging group identifier as *1234* for the ASN paging controller service:

```
paging-group id 1234
```

peer-asngw

Configures the addresses of trusted anchor ASN-GW peers. These are the peers with which a specified ASN Paging Controller and Location Registry service will allow R4 control and data path registration.

Product

ASN PC-LR

Privilege

Administrator

Syntax

[no] peer-asngw address *ip_address*[**id** *<MAC>* | **mode** [*legacy* | *non-legacy*]]

no

Removes the configured peer anchor ASN GW from a specific ASN PC/LR service's trusted peer list.

address *ip_address*

Specifies the IP address of the anchor ASN GW which is added as a trusted peer with the ASN PC/LR service in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to create trusted peer anchor ASN GWs with a specific ASN PC/LR service to establish R4 control and data path registration.
There is support for 6-byte ASNPC ID in the source or destination ID TLV, and for the Anchor GW and Authenticator IDs.
On receipt of an idle mode entry request message, the ASN PC/LR service checks the anchor DPF/authenticator. If the Anchor DPF/Authenticator ASN GW address received in the idle mode entry request message is not there, (or not configured in the peer list), the ASN PC/LR service sends the idle mode entry response message with a Failure Indication TLV with an unspecified error code.
Configure a maximum of 32 ASN GWs with this command.

Example

The following command adds the anchor ASN GW with an IP address of *10.2.3.4* as a trusted peer within an ASN PC service.

```
peer-asngw address 10.2.3.4
```

peer-asnpc

Configures the peer Anchor Paging Controller(s) in this ASN PC/LR service.

Product

ASN PC-LR

Privilege

Administrator

Syntax

[no] peer-asnpc [id < *mac_address*> **ip-address** < *ip_address* >]

no

Removes the configured peer ASN PC/LR MAC address and IP address as the trusted peer anchor ASN PC/LR.

id *mac_address*

Specifies the MAC address of the trusted peer system running the ASN paging controller and location registry service.
mac_address is the 6-byte MAC address of the paging controller (trusted R4 ASNGW peer) in standard (IEEE 802) format in six groups of two hexadecimal digits, separated by hyphens (-) or colons (:).

ip-address *ip_address*

Specifies the IP address of the trusted peer system running the ASN paging controller and location registry service in IPv4 dotted-decimal notation.

Usage

Use this command to configure the trusted peer anchor paging controller for ASN paging controller service. This command provides the input for the internal mapping from PC ID to IP address that is needed to forward the Location Update request from an Anchor PC to the current Anchor PC during PC relocation.

Example

The following command sets the peer AS NPC id to *01:23:45:67:89:ab* in colon (:) separated format and the IP address of the paging controller to 1.1.1.1:

```
peer-asnpc id 01:23:45:67:89:ab ip-address 1.1.1.1
```

policy overload

Configures traffic overload policy to control congestion in this service.

Product

ASN PC-LR

Privilege

Administrator

Syntax

```
policy overload { drop | reject }

default policy overload
```

default

Sets the traffic overload policy action to reject in this service.

drop

Specifies that the system is to drop incoming packets containing new session requests. Default: disabled

reject

Specifies that the system processes new session request messages and responds with a reject message. Default: enabled

Usage

Configure congestion policies at the service-level. When congestion control functionality is enabled at the service level, these policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

Example

The following command configures an overload policy of reject for this ASN PC service:

```
policy overload reject
```

retransmission-timeout

Configures the amount of time that must pass before the system re-attempts to send R6 control packets to the BS.

Product

ASN PC-LR

Privilege

Administrator

Syntax

retransmission-timeout < *duration* >

[no | default] retransmission-timeout

default

Sets the timeout duration to 3 seconds for retransmission of R6 control packets.

no

Disables or removes the configured timeout duration for retransmission of R6 control packets.

duration

Specifies the maximum time (in seconds) for the ASN paging controller service to wait for a response from the BS before it a) attempts to communicate with the BS again (if the system is configured to retry the BS), or b) marks the BS as unreachable.
duration is an integer from 1 through 1000. Default: 3

Usage

Use this command in conjunction with the **max-retransmission** command to configure the ASN paging controller services behavior when it does not receive a response from a particular BS.
Use the **no retransmission-timeout** command to delete a previously configured timeout value. If, after deleting the lifetime setting you desire to return the lifetime parameter to its default setting, use the **default retransmission-timeout** command.
The chassis is shipped from the factory with the retransmission timeout set to 3 seconds.

Example

The following command configures a retransmission timeout value of 5 seconds:

```
retransmission-timeout 5
```

The following command deletes a previously configured retransmission-timeout setting:

setup-timeout

Configures the amount of time for the ASN paging controller service to set up a connection with the BS before it marks the BS as unreachable.

Product

ASN PC-LR

Privilege

Administrator

Syntax

setup-timeout *duration*

default setup-timeout

default

Sets the timeout to 60 seconds to set up a connection with BS.

duration

Specifies the maximum allowable time (in seconds) for the ASN paging controller service to set up the R6 connection with BS before it marks the BS as unreachable.
duration is an integer between 1 and 100000. Default: 60

Usage

Use this command to configure the maximum timeout duration to setup an R6 connection with BS. This command supersedes the duration set through the **max-retransmission** and **retransmission-timeout** commands for R6 connection.

Example

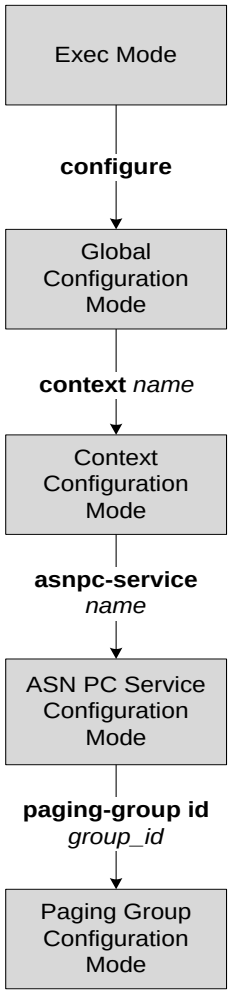
The following command configures an ASN paging controller service to mark a BS after waiting for *100* seconds before it marks it as unreachable:

```
setup-timeout 100
```

Chapter 28
ASN Paging Group Configuration Mode Commands

Use the Paging Group Configuration Mode to create and manage Paging Agents for the paging and location register controller within the Access Service Network Paging Controller and Location Registry (ASN PC-LR) service.

Important: This functionality is still in development stage.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

paging

Configures the paging parameters within the paging group for PC-LR functionality.

Product

ASN PC-LR

Privilege

Administrator

Syntax

paging { cycle *cycle_value* **| interval** *interval_value* **| node id** *mac_address* **address***ip_address* **| offset algorithm uniform start** *start_value* **increment** *inc_value* **count** *count_value* **}**

no paging { cycle | node id *mac_address* **| offset }**

no

Disables the configured paging parameters within this paging group.

cycle *cycle_value*

Specifies the cycle in which the paging message is transmitted within the paging group as an integer from 0 through 65535.

interval *interval_value*

Specifies the maximum duration in frames of Paging Listening Interval; used in calculation of Paging Listening Interval.
interval_value must be an integer from 1 through 5.

node id *mac_address* **address** *ip_address*

id *mac_address*: Configures the MAC address of the node in the paging group.
mac_address must be in one of the following formats:
nn:nn:nn:nn:nn:nn or nn-nn-nn-nn-nn-nn
address *ip_address*: Specifies the IP address of the node in IPv4 dottted-decimal or IPv6 colon-separated notation.

Important: Configure up to 128 paging nodes per paging group.

offset algorithm uniform start *start_value* **increment** *inc_value* **count** *count_value*

start *start_value*: Specifies the starting value of the available offset as an integer from 0 through 65535.
increment *inc_value*: Specifies the distance between two offsets as n integer from 0 through 65535.
count *count_value*: Specifies the number of offsets available as an integer from 0 through 65535.
Offsets are uniformly load balanced across the available range. For this configuration:
paging offset algorithm uniform start *10* **increment** *10* **count** *4*
the following occurs:
if MS1, MS2,...MS100, perform IM-Entry, then offset assigned: MS1=10, MS2=20, MS3=30, MS4=40, MS5=10, MS6=20, etc.

Usage

Use this command to define the paging behavior of a paging group. There must be only one instance of paging parameters per paging group.

Example

The following example configures the paging cycle for a paging group to *10*.

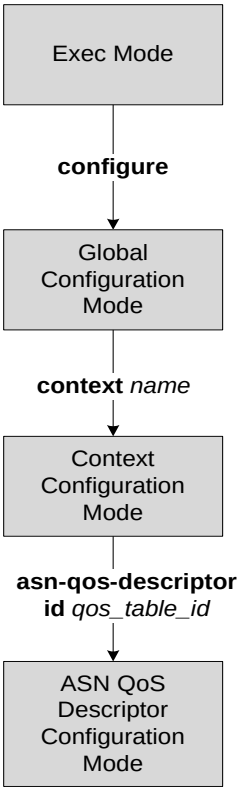
```
paging cycle 10
```

The following example configures a paging node in the group:

```
paging node id 00:05:47:00:37:44 address 12.345.76.789
```

Chapter 29
ASN QoS Descriptor Configuration Mode Commands

Use the ASN QoS Descriptor Configuration mode to create and manage the Quality of Service Descriptor table for ASN-GW service subscribers.



dscp

Configures DSCP marking of IP packets received on the ASN-GW on a service flow basis.

Product

ASN-GW

Privilege

Administrator

Syntax

```
dscp [ be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 |
af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef ]
```

be

Best effort. This is the default.

af11 through af43

Specifies that the DSCP marking is AFnn.

ef

Specifies that the DSCP marking is EF.

Usage

DSCP marking can be done via AAA or the CLI. From the AAA, it is received as part of the QoS descriptor. In the CLI, the DSCP value is configured as part of the asn-qos-descriptor.

Example

The following example shows the inclusion of DSCP marking in the command.

```
asn-qos-descriptor id 100 dscpaf21
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

global-service-class-name

Configures the global service class name within a QoS descriptor table.

Product

ASN-GW

Privilege

Administrator

Syntax

global-service-class-name *svc_class_name*

no global-service-class-name

no

Deletes the configured global service class name from this QoS descriptor table.

svc_class_name

Specifies the global service class name in QoS descriptor table an alphanumeric string of 6 characters.

Usage

Use this command to specify the global service class name (as per IEEE 802.16e standard) within a QoS descriptor table for an ASN-GW service.
The global service class name is similar in function to the Service Class Name except that (1) it may not be modified by a BS, (2) it remains consistent among all BSs, and 3) it is based on a rules-based naming system and contains referential QoS parameter codes.

Example

The following command specifies the global service class name *g_svc1* in an ASN QoS descriptor table:

```
global-service-class-name g_svc1
```

schedule-type

Configures the type of data delivery service identifier/type for an ASN-GW service.

Product

ASN-GW

Privilege

Administrator

Syntax

schedule-type be [max-sustained-traffic-rate *max_sust_traffic_rate* **| traffic-priority** *priority_value* **] +**

schedule-type ert-vr min-reserved-traffic-rate *min_resd_traffic_rate* **max-latency** *dur_ms* **unsolicited-grant-interval** *dur_ms* **[max-sustained-traffic-rate** *max_sust_traffic_rate* **| max-traffic-burst** *burst_size* **| tolerated-jitter** *dur_ms* **| traffic-priority** *priority_value* **] +**

schedule-type nrt-vr min-reserved-traffic-rate *min_resd_traffic_rate* **[max-sustained-traffic-rate** *max_sust_traffic_rate* **| max-traffic-burst** *burst_size* **| traffic-priority** *priority_value* **] +**

schedule-type rt-vr min-reserved-traffic-rate *min_resd_traffic_rate* **max-latency** *dur_ms* **unsolicited-polling-interval** *dur_ms* **[max-sustained-traffic-rate** *max_sust_traffic_rate* **| max-traffic-burst** *burst_size* **| traffic-priority** *priority_value* **] +**

schedule-type ugs max-sustained-traffic-rate *max-latency* **max-latency** *dur_ms* **unsolicited-grant-interval** *dur_ms* **[sdu-size** *sdu_size* **| tolerated-jitter** *dur_ms* **| traffic-priority** *priority_value* **| min-reserved-traffic-rate** *min-latency* **] +**

default schedule-type

default

Configures the data delivery service type to Best Effort (BE) service for a specific ASN-GW service.

be

Configures the data delivery service type to Best Effort (BE) service for a specific ASN-GW service.

ert-vr

Configures the data delivery service type to Extended Real-Time Variable Rate (ERT-VR) service for a specific ASN-GW service.

nrt-vr

Configures the data delivery service type to Non-Real-Time Variable Rate (NRT-VR) service for specific ASN-GW service.

rt-vr

Configures the data delivery service type to Real-Time Variable Rate (RT-VR) service for a specific ASN-GW service.

ugs

Configures the data delivery service type to Unsolicited Grant Service (UGS) for a specific ASN-GW service.

max-sustained-traffic-rate *max_resd_traffic_rate*

Specifies the maximum sustained traffic rate in bits per second, reserved for a service flow as n integer from 0 through 65535. Maximum latency set to zero means no commitment is available for this service flow.

max-latency *dur_ms*

Specifies the maximum interval (in milliseconds) between the receipt of a packet to a BS or an SS on its network interface/Convergence Sublayer (CS), and the arrival of a packet to its RF interface or the peer device. This value represents a service commitment.
dur_ms is an integer from 0 through 65535. Maximum latency set to zero means no commitment is available for this service flow.

min-reserved-traffic-rate *min_resd_traffic_rate*

Specifies the minimum traffic rates in bits per second, reserved for a service flow as an integer from 0 through 65535. A minimum reserved traffic rate set to zero means no minimum traffic rate reservation is required for this service flow. Default: 0 (disabled)

max-sustained-traffic-rate *max_sust_traffic_rate*

Configures the maximum sustained traffic rate in bits per second for traffic schedule as an integer from 1 through 65535.

max-traffic-burst *burst_size*

Specifies the maximum burst size in bits that must be maintained for the service as an integer from 0 through 65535. A maximum traffic burst set to zero means no maximum traffic burst reservation is required for this service flow. Default: 0 (disabled)

sdu-size *sdu_size*

Specifies the length of the Service Data Unit (SDU) in bytes for a fixed-length SDU service flow as an integer from 1 through 65535. Default: 49

Important: Use this parameter only if packing is on and the service flow is carrying fixed-length SDUs.

tolerated-jitter *dur_ms*

Specifies the maximum delay variation (jitter in milliseconds) allowed for the connection as an integer from 1 through 65535.

traffic-priority *priority_value*

Specifies the traffic priority as an integer from 0 through 7. Default: 0 (disabled)

unsolicited-grant-interval *dur_ms*

Specifies the nominal interval (in milliseconds) between successive data grant opportunities for this service flow as n integer from 1 through 65535.

unsolicited-polling-interval *dur_ms*

Specifies the maximum nominal interval (in milliseconds) between successive polling grants opportunities for this service flow as an integer from 1 through 65535.

Usage

Use this command to configure type of data delivery service identifier within ASN-GW service.

Important: Only one data delivery service type, **be**, **ert-vr**, **rt-vr**, **nrt-vr**, or **ugs** is allowed within an ASN-GW service.

Example

The following command configures the data delivery service type to Best Efforts (BE) service for an ASN-GW service:

```
default schedule-type
```

service-class-name

Configures the Service Class Name name within a specific QoS descriptor table.

Product

ASN-GW

Privilege

Administrator

Syntax

service-class-name *svc_class_name*

no service-class-name

no

Deletes the configured global service class name from this QoS descriptor table.

svc_class_name

Specifies the service class name in a QoS descriptor table as an alphanumeric string of 2 through 128 characters.

Usage

A service class name is a group of QoS parameters defined at the BS that can be referenced by a service flow to apply certain QoS parameters. Use this command to specify a service class name (per IEEE 802.16 standard) within a specific QoS descriptor table for an ASN-GW service

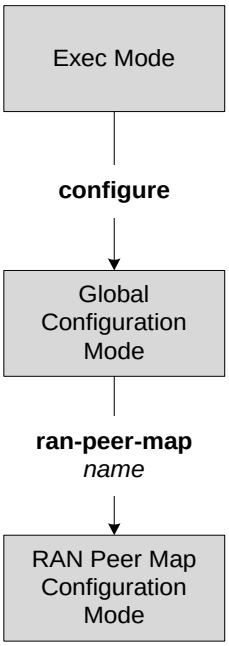
Example

The following command specifies the service class name *ASN_Serv_class1* in a ASN QoS descriptor table:

```
service-class-name ASN_Serv_class1
```

Chapter 30
ASN RAN Peer Map Configuration Mode Commands

Use the RAN Peer Map Configuration Mode to create and manage global mapping tables of Radio Access Network base station peers.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

ran-peer

Configure the MAC and IP addresses of the base station peers you are adding to this map.

Product

ASN-GW

Privilege

Administrator

Syntax

[no] ran-peer id *mac_address* **address** *ip_address* **[mode{non-legacy | legacy}]**

no

Removes the base station peer entry from this map.

id *mac_address* **address** *ip_address*

id *mac_address*: Configures the MAC address of the base station peer in this map.
mac_address must be in one of the following formats:
nn:nn:nn:nn:nn:nn or nn-nn-nn-nn-nn-nn
address *ip_address*: Specifies the IP address of the base station peer in IPv4 dotted-decimal or IPv6 colon-separated notation.
mode {non-legacy | legacy}: Default mode is non-legacy.

Usage

Use this command to add base station peers to this peer map.

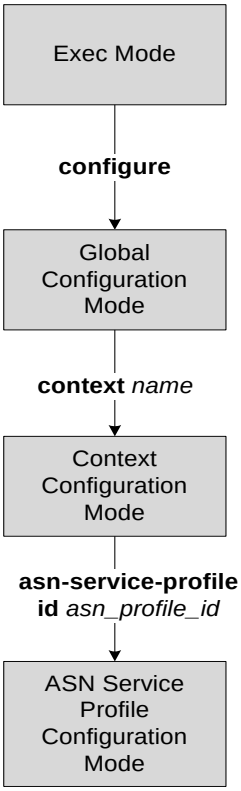
Example

The following command adds a base station peer to this map:

```
ran-peer id 00:05:47:00:37:44 address 12.345.76.789
```

Chapter 31
ASN Service Profile Configuration Mode Commands

Use the ASN Service Profile Configuration Mode to create and manage the service profiles table for the ASN-GW service subscribers within the current context.



downlink-classifier

Specifies which classifier to match for traffic flow in the downlink direction for subscribers in this service.

Product

ASN-GW

Privilege

Administrator

Syntax

[no] downlink-classifier class-map < *class_map_name* > [**id** < *0-65535* >] [**priority** < *0-255* >] **[action { permit | deny }]**

no

Deletes the configured class map for this traffic flow in the ASN-GW service.

class-map *class_map_name*

Associates an existing Class-Map in the destination context to this traffic flow.
For example:

- For downlink-classifier class-map c4, an id of 1 is generated or assigned.
- For downlink-classifier class-map c5, an id of 2 is generated or assigned.
- For downlink-classifier class-map c6, an id of 3 is generated or assigned.

Refer to the *Class-Map Configuration Mode Commands* chapter for additional information on configuring the class maps.

id < *0-65535* >

Assure that **id** is unique in an asn-service-profile. If you do not configure the classier id, the sorted classifier name order is assigned as *id*.

priority < *0-255* >

Default: 0

0 = minimum, 255 = maximum

Usage

Use this command to configure classifier for downlink traffic with a configured Class-Map for the ASN-GW service subscribers.
You can configure a maximum of four class-maps in one ASN-GW service profile.
Access Class-Map Configuration Mode through the Context Configuration Mode.

Example

The following command applies the Class-Map *class_1* to this traffic:

```
downlink-classifier class-map class_1
```

downlink-qos-id

Specifies the QoS table identifier to traffic flowing in the downlink direction for subscribers in this service.

Product

ASN-GW

Privilege

Administrator

Syntax

downlink-qos-id *< qos_table_id >*

[no] downlink-qos-id

no

Deletes the configured class map for this traffic flow in the ASN-GW service.

qos_table_id

Associates an existing ASN QoS descriptor identifier in the source context to this traffic flow.
Refer to the *ASN QoS Descriptor Configuration Mode Commands* chapter of this reference for additional information on configuring QoS descriptor table identifiers.

Usage

Use this command to apply a QoS identifier for downlink traffic with a configured ASN QoS descriptor table identifier for the ASN-GW service subscribers.
Configure only one QoS identifier per ASN-GW service profile.
Access ASN QoS Descriptor Configuration Mode through Context Configuration Mode.

Example

The following command applies the QoS table identifier *123* to this traffic:

```
downlink-qos-id 123
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

uplink-classifier

Specifies which classifier to match for traffic flow in the uplink direction for subscribers in this service.

Product

ASN-GW

Privilege

Administrator

Syntax

[no] uplink-classifier class-map < *class_map_name* > [**id** < *0-65535* >] [**priority** < *0-255* >] **[action { permit | deny }]**

no

Deletes the configured class map for this traffic flow in the ASN-GW service.

class-map *class_map_name*

Specifiesan existing Class-Map in the destination context to this traffic flow. For example:

- For uplink-classifier class-map c1, an id of 1 is generated or assigned.
- For uplink-classifier class-map c2, an id of 2 is generated or assigned.
- For uplink-classifier class-map c3, an id of 3 is generated or assigned.

Refer to the *Class-Map Configuration Mode Commands* chapter for additional information on configuring class maps.

id < *0-65535* >

Assure that **id** is unique in an asn-service-profile. If you do not configure the classier id, the sorted classifier name order is assigned as *id*.

priority < *0-255* >

Default: 0

0 = minimum, 255 = maximum

Usage

Use this command to configure classifier for uplink traffic with a configured Class-Map for the ASN-GW service subscribers.
Configure a maximum of 4 class-maps per ASN-GW service profile.
Access Class-Map Configuration Mode through Context Configuration Mode.

Example

The following command applies the Class-Map *class_1* to this traffic:

```
uplink-classifier class-map class_1
```

uplink-qos-id

Specifies the QoS table identifier to the traffic flow in the uplink direction for subscribers in this service.

Product

ASN-GW

Privilege

Administrator

Syntax

uplink-qos-id *qos_table_id*

[no] uplink-qos-id

no

Deletes the configured class map for this traffic flow in the ASN-GW service.

uplink_qos_id

Associates an existing ASN QoS Descriptor Identifier in the source context to this traffic flow.
Refer to the *ASN QoS Descriptor Configuration Mode Commands* chapter for additional information on configuring the QoS descriptor table identifier.

Usage

Use this command to apply a QoS identifier for uplink traffic with a configured ASN QoS Descriptor Table Identifier for the ASN-GW service subscribers.
Configure only one QoS identifier per ASN-GW service profile.
Access ASN QoS Descriptor Configuration Mode through Context Configuration Mode.

Example

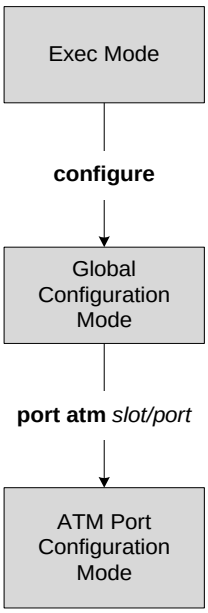
The following command applies the QoS table identifier *123* to this traffic:

```
uplink-qos-id 123
```

Chapter 32
ATM Port Configuration Mode Commands

The Asynchronous Transfer Mode (ATM) port configuration mode provides the commands to create, configure, bind, and manage the ATM ports on line cards that support ATM, such as the ATM/POS OC-3 single-mode and multi-mode optical line cards.

Important: Before using these commands, card framing should be configured for either SDH or SONET with the framing command described in the *Card Configuration Mode* chapter.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

clock-source

This command sets the source of the port's transmit clock.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
clock-source { internal-timing | loop-timing }

default clock-source
```

default

Using this command combination sets the port clock source to internal timing.

internal-timing

Sets the port clock to derive timing from the recovered receive clock.

loop-timing

Sets the port clock to transmit in sync with the system timing.

Usage

Use this command for either SONETports on the SGSN.

Important: This command is only available for releases 8.1 or higher.

Example

The following command resets the transmit clock source to internal timing.

```
default clock-source
```

description

Defines descriptive text that provides useful information about the port.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

description *text*

no description

no

Erases the port's defined description from the configuration file.

text

text must be a string of 1 to 79 alphanumeric characters with no spaces or a string within double quotes that includes printable characters. The description is case-sensitive.

Usage

Set the description to provide helpful information, for example the port's primary function, services, end users. Define any information, the only limit is the number of characters.

Example

The following example sets a port description that will read in the configuration file:

description *samplePortDescriptiveText*

The following example sets a port description that will be easy to read because it retains the spaces between words:

description *"This is a sample description"*

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

line-timing

This command enables the SPIO to recover transmit timing source via the line attached to the selected port. By default, line-timing is not enabled.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] line-timing
```

no

Disables line-timing as the source for the transmit clock.

Usage

The port must be enabled (**no shutdown**) to enable recovery of timing source via the line. As well, the card's slot number must be entered in the **recover line#** command in the BITS port configuration mode.

Example

Disable configured line-timing as the clock source for this port.

```
no line-timing
```

loopback

Enables/disables loopback and configures the type of loopback mode used for diagnostic testing.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

loopback { ds1-e1-diag | ds1-e1-line | none | sonet-sdh-diag | sonet-sdh-line }

ds1-e1-diag

Enables a system generated diagnostic lookback signal at the DS1/E1 layer.

ds1-e1-line

Loops back a network diagnostic signal at the DS1/E1 layer.

none

Stops diagnostic loopback signalling.

sonet-sdh-diag

Enables a system generated diagnostic lookback signal at the SONET/SDH layer.

sonet-sdh-line

Loops back a network diagnostic signal at the SONET/SDH layer.

Usage

Setup diagnostic loopback signals for troubleshooting purposes.

Example

Use the following command to setup loopback diagnosis:

```
loopback ds1-e1-diag
```

Use the following command to disable loopback:

```
loopback none
```

preferred slot

This command identifies which card in a chassis assumes revertive (redundancy auto-recovery) functionality when the slot/port being configured go down.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

preferred slot *slot#*

[default | no] preferred slot

default

Default: non-revertive operation.
Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a port switch to command to return service to the original port.

no

Disables revertive, or auto-recovery, operation for the port.

slot#

Identifies the physical slot in the chassis where the preferred line card is installed.

Usage

This command enables or disables revertive port redundancy. So after a port failover, when the original port is restored to service (i.e. link up) the system will return service to that port automatically.
This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual LCs or SPIO cards. For example, ports 1 through 4 could be configured as “preferred” on the LC in slot 17 while ports 5 through 8 are “preferred” on the LC in slot 33. In this scenario, both LCs would be in an Active operational state while still providing LC and port redundancy for the other.
Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a port switch command to return service to the original port.

Example

The following commands sets revertive port redundancy for ports on the card in slot 17:

```
preferred slot 17
```

pvc

This command creates a Permanent Virtual Connection (PVC), including the definition of the associated Virtual Path Identifiers (VPI) and Virtual Connection Identifiers (VCI) for the PVC. By defining a PVC, this command enters into PVC configuration mode. The ATM port supports a maximum of 256 PVC definitions.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

[no] pvc vpi *vpi#* **vci** *vci#* **[type { aal2 [cps-payload-size** *cps_payload_value* **| aal5 }]] [-noconfirm]**

no

Deletes the PVC's entry from the configuration.

vpi *vpi#*

VPI identifies a unique path to a destination point in the ATM portion of the network. The VPI and the VCI combine to create the PVC between the MS and the destination point. *vpi#* must be an integer, 0 to 255.

vci *vci#*

VCI identifies a unique virtual circuit within the associated VPI. *vci#* must be an integer, 0 to 65535.

type

This keyword is used to define the type of PVC as AAL2 or AAL5 for HNB-GW service configuration within the associated VPI and VCI.

aal2

This keyword is used to define the type of PVC as AAL2 for HNB-GW service configuration within the associated VPI and VCI.

aal5

This keyword is used to define the type of PVC as AAL5 for HNB-GW service configuration within the associated VPI and VCI.

cps-payload-size *cps_payload_value*

This keyword configures the Common Part Sublayer (CPS) payload in Bytes for AAL2 type of PVC within the associated VPI. CPS payload is carried out by the AAL2 protocol over ATM. During the call, the payload size is negotiated between HNB-GW and MSC. Default size for payload is 64 but values may range from 1 to 64 Bytes. This command makes the operator to choose the size dynamically
The CPS payload size dynamically configured for per PVC. If user is not providing the CPS payload size then default value of 64 Bytes is considered else user provided value is taken.
cps_payload_value is the value of CPS payload in Bytes and must be an integer between 1 through 64.

-noconfirm

Specifies that the command must execute without any additional prompt and confirmation from the user.

Usage

Creates a virtual circuit between two specific points that the carrier will use repeatedly.
This command is used to define the type of PVC as AAL2 or AAL5 for HNB-GW service configuration. It also configures the CPS payload which is carried out by the AAL2 protocol over ATM. During the call, the payload size is negotiated between HNB-GW and MSC. Default size for payload is 64 but values may range from 1 to 64 Bytes. This command makes the operator to choose the size dynamically.
This command configures the type of PVC to ATM Adaptation Layer2 (AAL2) or ATM Adaptation Layer5 (AAL5) for ATM traffic between HNB-GW and MSC. It also enables the operator to configure the Common Part Sublayer (CPS) payload for AAL2 protocol over ATM for HNB-GW session between MSC and HNB-GW.

Example

Define a PVC with VPI 2 and VCI 353.

```
pvc vpi 2 vci 353
```

Following command configures the PVC type as AAL2 with VPI as *2* and VCI as *353*. It also configures the CPS payload to *45* bytes over the ATM during the call.

```
pvc vpi 2 vci 353 type aal2 cps-payload-size 45
```

shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, this command with the **no** keyword enables the port.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] shutdown
```

no

Enables the port's administrative state. When this command is omitted from the configuration, the card is shutdown (removed from service).

Usage

Shut down a port prior to re-cabling and/or other maintenance activities. This is the default state of each port upon installation and initial configuration.
This command with the **no** keyword is *required* to bring a port into active service.

Example

The following command enables the port for service:

```
no shutdown
```

The following command disables the port and takes it out of service:

```
shutdown
```

snmp trap link-status

Enables/disables the generation and sending of an SNMP (notification) trap when the port experiences a change of state (up or down).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] snmp trap link-status
```

no

Disables the sending of traps for link-status changes.

Usage

Enable the sending of link-status change traps for this port if there is a monitoring facility that can use the information or if there are troubleshooting activities in progress.

Example

Use the following command to send SNMP link-status traps for this port:

```
snmp trap link-status
```

Use the following command to disable the sending SNMP link-status traps for this port:

```
no snmp trap link-status
```

threshold high-activity

Configures the port's high and low activity thresholds.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

threshold high-activity *high_thresh* **[clear** *low_thresh* **]**

default threshold high-activity

default

Restores both port high-activity thresholds to the system default of 50 percent.

high_thresh

Default: 50
Sets the threshold for the highest percentage of port activity that must be met or exceeded, within the polling interval, to generate an alert or alarm.
high_thresh_% can be configured to any integer value between 0 and 100.

clear *low_thresh*

Default: 50
Sets the threshold for the lowest percentage level of port activity that must be met to generate and send a clear alarm. If port activity does not drop to or below this threshold then the alarm is maintained.
low_thresh_% can be configured to any integer value between 0 and 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

High port activity thresholds generate alerts or alarms based on the utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis.
Alerts or alarms are triggered for high port activity based on the following rules:

- **Enter condition:** Actual percent utilization of a port > High Threshold
- **Clear condition:** Actual percent utilization of a port < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command in the *Global Configuration Mode Commands* chapter of this reference to configure the polling interval and the **threshold monitoring** command in this chapter to enable thresholding for this value.

Example

The following command configures a high port utilization threshold of 70 percent and a low threshold of 50 percent for a system using the Alarm thresholding model:

```
threshold high-activity 70 clear 50
```

threshold monitoring

Enables thresholding for port-level values.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] threshold monitoring
```

default

Restores the system default to disable threshold monitoring for port-level values.

no

Disables threshold monitoring for port-level values. This is the default setting.

Usage

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high-activity) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the SNMP MIB Reference.

The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.
- **Alarm System:** High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists and/or a condition clear alarm is generated.

"Outstanding" alarms are reported to through the system's alarm subsystem and are viewable through the system's CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

Table 10. Thresholding Reporting Mechanisms by Model

Model	SNMP Traps	Logs	Alarm System
Alert	X	X	
Alarm	X	X	X

This command enables thresholding for port-level values. Refer to the sections covering **threshold high-activity**, **threshold rx-utilization,** and **threshold tx-utilization** commands in this chapter for information on configuring these values. In addition, refer to the **threshold poll** command in the *Global Configuration Mode Commands* chapter of this reference for information on configuring the polling interval over which these values are monitored.

threshold rx-utilization

Configures thresholds for receive-port utilization.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold rx-utilization *high_thresh* **[clear** *low_thresh* **]**

default threshold rx-utilization

default

Restores both rx-utilization thresholds to the system default of 80 percent.

high_thresh

Default: 80
The high threshold receive port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
The percentage can be configured to any integer value between 0 and 100.

clear *low_thresh*

Allows the configuration of the low threshold.
Default: 80
The low threshold receive port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
The percentage can be configured to any integer value between 0 and 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis.

Important: Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive **or** transmit utilization threshold be configured.

Alerts or alarms are triggered for receive port utilization based on the following rules:

- **Enter condition:** Actual percent utilization of a port for received data > High Threshold

- **Clear condition:** Actual percent utilization of a port for received data < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the **threshold monitoring** command in this chapter to enable thresholding for this value.

Example

The following command configures a receive port high utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold rx-utilization 70 clear 50
```

threshold tx-utilization

Configures thresholds for transmit port utilization.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold tx-utilization *high_thresh* **[clear** *low_thresh* **]**

default threshold tx-utilization

default

Restores the port tx-thresholds to their system defaults of 80 percent.

high_thresh

Default: 80
The high threshold transmit port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
The percentage can be configured to any integer value between 0 and 100.

clear *low_thresh*

Allows the configuration of the low threshold.
Default: 80
The low threshold transmit port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
The percentage can be configured to any integer value between 0 and 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis.

Important: Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive **or** transmit utilization threshold be configured.

Alerts or alarms are triggered for transmit port utilization based on the following rules:

- **Enter condition:** Actual percent utilization of a port for transmit data > High Threshold

- **Clear condition:** Actual percent utilization of a port for transmit data < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the **threshold monitoring** command in this chapter to enable thresholding for this value.

Example

The following command configures a transmit port high utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold tx-utilization 70 clear 50
```

toh-sdsf

Enable/disable line SDSF BER thresholds and configure the line transport overhead (TOH) signal degrade and signal failure (SDSF) bit error rate (BER) threshold.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

toh-sdsf *toh_value*

default toh-sdsf

default

Resets the default which disables this threshold.

toh_value

To facilitate configuration the SD and SF rates have been combined into a single setting. .

- 0: Disabled
- 1 -1.E-04
- 2 - 1.E-05
- 3 - 1.E-06
- 4 - 1.E-07
- 5 - 1.E-08
- 6 - 1.E-09
- 7 - 1.E-10
- 8 - 1.E-11

Usage

This command is typically configured in combination with configuring APS/MSP redundancy for the line card - see the **aps** and the **redundancy** commands documented in the *Card Configuration Mode Commands* chapter..

This command can be used to configure the line threshold whether the port is active or standby and sets a standard option for the paired values of the line's signal degrade and signal failure (SDSF) BER.

The SD is kept at a value of 100 erroredBits/sec less than the corresponding value of the SF. So if the SD threshold is configured at 1 error in every 100000 bits/sec, then the SF threshold automatically becomes 1 error in every 1000 bits/sec.

The port will go operationally down as soon as the SD threshold is crossed.

Example

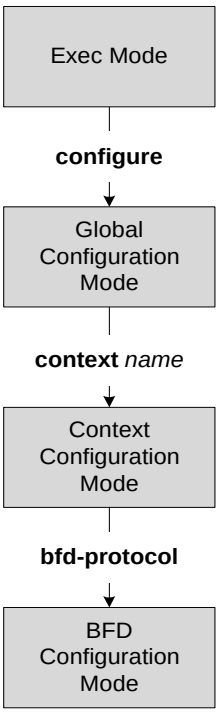
Set

```
toh-sdsf 1
```

Chapter 33
BFD Configuration Mode Commands

The BFD Configuration Mode manages the protocol settings for Bidirectional Forwarding Detection (BFD).

BFD provides a low-overhead, short duration method of detecting failures in the forwarding path between two BGP adjacent routers, including the interfaces, data links, and forwarding plane. BFD must be enabled on both routers. The ASR 5000 supports BFD on Layer 3 clients only in asynchronous mode with optional Echo functionality.



bfd multihop-peer

Configures parameters for any multihop-BFD sessions with the same destination address. If these parameters are not configured via this command, MH-BFD sessions with the same destination address will be in the Admin-down state.

Product

All

Privilege

Security Administrator, Administrator

Syntax

bfd multihop-peer *dst-ip-address* **{ authentication { md5 | meticulous-md5 | meticulous-sha1 plain-text | sha1 } { encrypted** *password-string* **| password** *password-string* **} | interval** *tx_interval* **min_rx** *rx_interval* **multiplier** *value* **}**

no bfd multihop-peer *dst-ip-address* **authentication**

---

no

Removes all the parameters for the MH-BFD destination address and if there are any sessions with the same destination address, those sessions will go to Admin-down state.

---

dst-ip-address

Specifies the destination address of the BFD enabled peer in IPv4 dotted-decimal or IPv6 colon-separated notation. This destination address must have been previously configured via the **ip route static bfd** commands in the Context Configuration mode.

---

authentication { md5 | meticulous-md5 | meticulous-sha1 plain-text | sha1

Specifies the method for authenticating all multihop BFD sessions to the specified peer. By default, authentication for Multihop-BFD sessions to a destination address is disabled. The authentication type options include:

- **md5** – Message Digest 5
- **meticulous-md5** – MD5 using a secret key and sequence numbers updated for every packet
- **meticulous-sha1** – SHA1 with sequence numbers updated for every packet
- **plain-text** – plain text (unencrypted)
- **sha1** – Secured Hash Algorithm 1

---

encrypted *password-string* **| password** *password-string*

Specifies the password for authentication of BFD sessions. The password must be the same between the peer neighbors for the BFD sessions to work. If the authentication password is configured incorrectly between peers, the BFD sessions to the destination address will not come UP. If the password is configured for BFD sessions that are already UP, BFD neighbors will be reset.

- **encrypted** *password-string*: Specifies the use of an encrypted password for authentication of BFD sessions as an alphanumeric string of up to 523 characters.
- **password** *password-string*: Specifies the use of a plain text password for authentication of BFD sessions as an alphanumeric string of 1 through 19 characters.

Important: The destination address and its transmit/receive intervals must be configured before the password is applied to any MH-BFD sessions at a destination address.

`interval` *`tx_interval`* **`min_rx`** *`rx_interval`* **`multiplier`** *`value`*

`interval` *`tx_interval`*: Specifies the transmit interval (in milliseconds) between BFD packets as an integer from 50 through 999. Default: 50
`min_rx` *`rx_interval`*: Specifies the receive interval (in milliseconds) between BFD packets as an integer from 50 through 999. Default: 50
`multiplier` *`value`*: Specifies the multiplier value sued to compute holddown as an integer from 3 through 50. Default: 3

Usage

Use this command to configure basic operating parameters between BFD enabled peers.

Example

```
bfd multihop-peer 10.2.3.4 authentication md5 encrypted 5-klm7783 bfd
multihop-peer 10.2.3.4 interval 100 min_rx 100 multiplier 5
```

bfd nbr-group-name

Configures BFD neighbor groups.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] bfd nbr-group-name *neighbor-group* **{ active-if-name** *if-name* **| passive-if-name** *if-name* **}** *gw-ip-address*

no bfd nbr-group-name *neighbor-group*

no

Removes all the parameters for the BFD neighbor group.

bfd nbr-group-name *neighbor-group*

Specifies an identifier for a BFD neighbor group as an alphanumeric string of 1 through 19 characters.

active-if-name *if-name* **| passive-if-name** *if-name*

Specifies the logical/physical interface associated with this BFD group.
active-if-name *if-name*: Specifies an active interface that notifies all passive interfaces in this group. There should be only one active interface in a group. *if-name* is a logical or physical interface specified as an alphanumeric string of 1 through 79 characters.
passive-if-name *if-name*: Specifies a passive interface that receives BFD notifications from the active interface in this group. *if-name* is a logical or physical interface specified as an alphanumeric string of 1 through 79 characters.

gw-ip-address

Specifies the gateway address of the BFD neighbor in IPv4 dotted-decimal or IPv6 colon-separated notation (optional CIDR notation).

Usage

Allow scaling of BFD sessions when a large number of logical interfaces are configured on a physical interface. A failure on the physical interface or a logical interface can be propagated to all passive interfaces in this group.

Example

```
bfd nbr-group-name bgpgroup132 active-if-name bgpif02
```

echo

Enables or disables BFD echo mode functionality. The Echo function tests the forwarding path on the remote system. Echo is only used for single hop BFD sessions

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] echo
```

no echo

Disables BFD echo functionality.

Usage

Use this function to send a stream of Echo packets that the other endpoint then sends back via its forwarding plane. Echo tests the forwarding path on the remote system.

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

slow-timers

Specifies the asynchronous mode control packet interval when Echo mode is enabled. In BFD asynchronous mode, BFD-enabled peers periodically send BFD Control packets to one another. If a number of those packets in a row are not received within the specified interval by the other peer, the session is declared to be down.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] slow-timers *timer-value*

no slow-timers

no

Disables previously specified BFD slow timers.

slow-timers *timer-value*

Specifies the BFD control packet interval (in milliseconds) for Echo mode as an integer from 1000 through 300000. Default: 2000

Usage

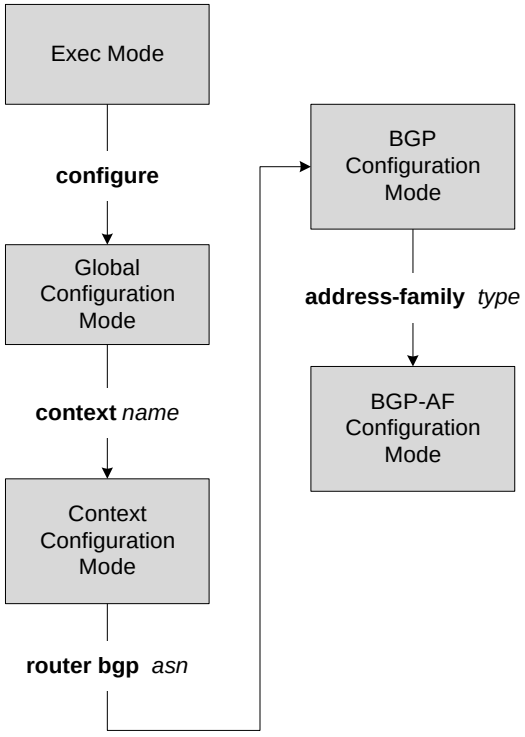
Use this command to configure the interval between BFD control packets sent between peers in Echo mode.

Example

```
slow-timers 10000
```

Chapter 34
BGP Address-Family (IPv4/IPv6) Configuration Mode Commands

The Border Gateway Protocol (BGP) Address-Family (IPv4/IPv6) Configuration Mode is used to configure the IPv4 and IPv6 address family information.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

maximum-paths

Controls the maximum number of parallel external BGP (eBGP) or internal BGP (iBGP) routes that can be installed in a routing table.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] maximum-paths { ebgp *num_paths* **| ibgp** *num_paths* **}**

no

Disables the above command.

maximum-paths ebgp *num_paths*

Specifies the maximum number of parallel External Border Gateway Protocol routes as an integer from 1 through 10.

maximum-paths ibgp *num_paths*

Specifies the maximum number of parallel Internal Border Gateway Protocol routes as an integer from 1 through 10.

Important: If configured under the router-bgp-mode, multipath is enabled only for the prefixes learnt in the default-vrf. There is no support for vpnv4 prefixes even though multipath is turned on for the default-vrf. If configured under the address-family-vrf-mode, multipath is enabled only for prefixes learnt in the vrf.

Usage

Use this command to forward packets over multiple paths. User can control the maximum number of parallel eBGP routes that can be installed in a routing table. Enabling multipath does not affect the best path selection in BGP. If multipath is enabled, all the paths with the same weight, local-preference, as-path length, origin, and multi-exit discriminator (MED) as the best path are added to the routing table.

Example

The following command disables forward of packets over multiple paths:

no maximum-paths ebgp

neighbor

Configures the IPv4/IPv6 Address Family for BGP routers that interconnect to non-broadcast networks.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] neighbor *ip_address* **{ activate | advertisement-interval** *adv_time* **| capability graceful-restart | default-originate [route-map** *map_name* **] | distribute-list** *dist_list* **{ in | out } | ebgp-multihop [max-hop** *number* **] encrypted password** *encryp_password* **fall-over bfd multihop | filter-list** *filt_list* **{ in | out } | max-prefix** *max_num* **[threshold** *thresh_percent* **] [warning-only] next-hop-self | password** *password* | **remote-as** *AS_num* **| remove-private-AS | restart-time** *rest_time* **| route-map** *map_name* **{ in | out} | send-community { both | extended | standard } | shutdown | srp-activated-soft-clear | timers { connect-interval** *connect_interval* **[keepalive-interval** *keepalive_interval* **holdtime-interval** *holdtime_interval* **[min-peer-holdtime-interval** *min_peer_hold_interval* **]] | keepalive-interval** *keepalive_interval* **holdtime-interval** *holdtime_interval* **{ connect-interval** *connect_interval* **| min-peer-holdtime-interval** *min_peer_hold_interval* **[connect-interval** *connect_interval* **] } } | update-source** *ip_address* **| weight value }**

no

Delete the specified parameter from the router configuration.

neighbor *ip_address*

Specifies the IP address of a BGP neighbor. *ip_address* must be in IPv4 dotted-decimal or IPV6 colon-separated notation.

activate

Enables the exchange of routes with this neighbor.

advertisement-interval *adv_time*

Specifies the minimum interval (in seconds) between sending BGP routing updates.
adv_time must be an integer from 0 through 600. Default: 30

capability graceful-restart

Configures graceful re-start attributes.

default-originate [route-map *map_name* **]**

Specifies the default originate routes to this neighbor
route-map *map_name*: Specifies the route-map that contains the criteria to originate default routes.
map_name must be the name of an existing route-map in the current context.

distribute-list *dist_list* **{ in | out }**

Filters updates to and from this neighbor based on a route access list. Default: No filtering is performed.
dist_list is the name or number of an existing route-access-list.
in: Indicates that incoming advertised routes should be filtered.
out: Indicates that outgoing advertised routes should be filtered.

ebgp-multihop [max-hop *number* **]**

Allows eBGP neighbors that are not on directly connected networks.
max-hop *number*: Specifies the maximum number of hops allowed to reach a neighbor as an integer from 1 through 255. Default hop count: 255

encrypted password *encryp_password*

Specifies the encrypted password that is used only inside configuration files. This is an alphanumeric string of 1 through 24 characters.

fall-over bfd multihop

Supports Bidirectional Forwarding Detection (BFD) multihop for fallover.

filter-list *filt_list* **{in | out}**

Establishes BGP filters based on an autonomous system (AS) path access list. *filt_list* is name of an existing AS path access list.
in: Indicates that incoming advertised routes will be filtered.
out: Indicates that outgoing advertised routes will be filtered.

max-prefix *max_num* **[threshold** *thresh_percent* **] [warning-only]**

Specifies the maximum number of prefixes accepted from this peer. When the maximum is exceeded the neighbor connection is reset. *max_num* is an integer from 1 through 4294967295. Default: No maximum prefix limit.
threshold *thresh_percent*: Specifies a percentage value of when the BGP table is full. When this value is reached peer warnings are sent to the neighbor. *thresh_percent* must be an integer from 1 through 100.
warning-only: Specifies that only a warning message is sent when the limit is exceeded. The neighbor connection is not reset

next-hop-self*ip_address*

Disables the next hop calculation for this neighbor.

password*password*

Sets a *password* expressed as an alphanumeric string of 1 through 24 characters.

remote-as *AS_num*

Specify the AS number of the BGP neighbor as an integer from 1 through 4294967295.

remove-private-AS

Removes the private AS number from outbound updates. Default: Do not remove the private AS number.

restart-time *rest_time*

Specifies the maximum time (in seconds) required to for neighbor to restart as an integer from 1 through 3600.

route-map *map_name* **{ in | out }**

Applies a route map to the neighbor. *map_name* must be the name of an existing route-map in the current context.
in: Indicates that the route map applies to incoming advertisements.
out: Indicates that the route map applies to outgoing advertisements.

send-community{ both | extended | standard }

Sends the community attributes to a peer router (neighbor).
both:Sends standard and extended community attributes
extended:Sends extended community attributes.
standard:Sends standard community attributes.

shutdown

Administratively shuts down this neighbor. This disables exchanging routes or configuring parameters for this neighbor.

srp-activated-soft-clear

Enables BGP updates when SRP-enabled resources are modified.

timers { [connect-interval *connect_interval* **] | [keepalive-interval** *keepalive_interval* **holdtime-interval** *holdtime_interval* **] }**

Sets BGP timers for the specified neighbor.
connect-interval *connect_interval*: Specifies the connect timer (in seconds) as an integer from 0 through 65535. The default is 60 seconds.
keepalive-interval *keepalive_interval*: Specifies the frequency (in seconds) at which the current BGP router sends keepalive messages to its neighbor. *keep_time* must be an integer from 0 through 65535. The default is 30 seconds.
holdtime-interval *holdtime_interval*: Specifies the interval (in seconds) the router waits for a keepalive message before declaring a neighbor dead. *hold_time* must be an integer from 0 through 65535. The default is 90 seconds.
min-peer-holdtime-interval *min_peer_hold_interval*: Specifies the minimum acceptable hold time (in seconds) from peer for a keepalive message before declaring a neighbor dead.
min_peer_hold_interval must be an integer from 0 through 65535. The default is 90 seconds.

update-source *ip_address*

Binds the specified IP address to the BGP socket that is used to communicate to the peer. *ip_address* is an IPv4 address in dotted-decimal notation.
In most cases you should set the update-source address to the address of the loopback interface in the current context. By doing this, the TCP connection does not go down until there is no route for the loopback address in the peering router.

weight *value*

Sets the default weight for routes from this neighbor as an integer from 0 through 65535. Default: 0

Usage

Use this command to set parameters for communication with a specified neighbor. The chassis supports a maximum of 64 peers per context.

Important: A remote AS number must be specified for a neighbor before other parameters can be configured.

Example

The following command specifies that the neighbor at the IP address *192.168.100.25* has an AS number of *2000*:

```
neighbor 192.168.100.25 remote-as 2000
```

The following command allows BGP neighbors that are a maximum of *27* hops away:

```
neighbor 192.168.100.25 ebgp-multihop max-hop 27
```

The following command sets the minimum interval between sending routing updates to 3 minutes (180 seconds):

```
neighbor 192.168.100.25 advertisement-interval 180
```

The following command sets the default weight for all routes from the specified neighbor to *100*:

```
neighbor 192.168.100.25 weight 100
```

network

Configures and specifies a network to announce via BGP.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] network *ip_address/mask* **[route-map** *map_name* **]**

no

Delete the specified network from the configuration for the BGP router.

network *ip_address/mask*

Specifies the IP address and netmask bits for the network to announce via BGP. *ip_address* is a network IP address in IPV4 dotted-decimal notation and *mask* is the number of subnet bits, representing a subnet mask in CIDR. These must be entered in the IPv4 dotted-decimal notation/subnet bits format.

route-map *map_name*

Filter routes through the specified route map before announcing the network. *map_name* specifies the name of the route-map to use as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to specify a network to announce via BGP.

Example

The following command announces the network *192.168.0.0* with a netmask of *16* via BGP:

```
network 192.168.0.0/16
```

The following command removes the network from the BGP router configuration:

```
no network 192.168.0.0/16
```

redistribute

Redistributes routes into BGP from another protocol as BGP neighbors.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] redistribute { connected | ospf | rip | static } [route-map *map_name* **]**

no

Remove the specified redistribution parameters from the BGP router configuration.

redistribute connected

Specifies that connected routes will be redistributed.

redistribute ospf

Specifies that Open Shortest Path First (OSPF) routes will be redistributed

redistribute rip

Specifies that Routing Information Protocol (RIP) routes will be redistributed. (RIP is not supported at this time.)

redistribute static

Specifies that static routes will be redistributed.

route-map *map_name*

Filters routes through the specified route map before redistribution. *map_name* specifies the name of the route-map to use as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to specify what routes this BGP router should redistribute into BGP.

Example

The following command redistributes OSPF routes after filtering them through the route map named *Map1*:

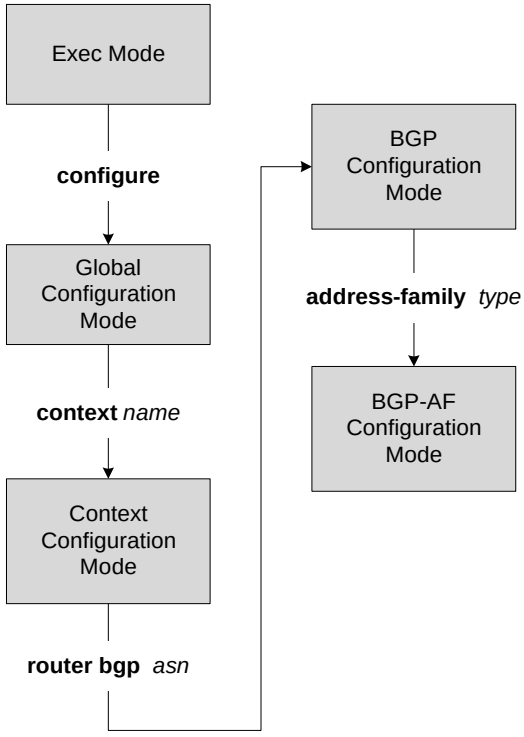
```
redistribute ospf route-map Map1
```

The following command removes the redistribution of OSPF routes from the router's configuration:

```
no redistribute ospf route-map Map1
```

Chapter 35
BGP Address-Family (VPNv4) Configuration Mode Commands

The Border Gateway Protocol (BGP) Address-Family (VPNv4) Configuration Mode is used to configure the VPNv4 address family information.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

neighbor

Configures the VPNv4 address family on BGP routers that interconnects to non-broadcast networks and enables the exchange of routing information with a peer router (neighbor).

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] neighbor *ip_address* **{ activate | send-community { both | extended | standard } }**

no

Delete the specified parameter from the router configuration.

neighbor *ip_address*

Specifies the IP address of the peer router (neighbor) in IPv4 dotted-decimal or IPv6 colon-separated notation.

activate

Enables the exchange of routing information with this neighbor.

send-community { both | extended | standard }

Sends the community attributes to a peer router (neighbor).
both: Sends standard and extended community attributes.
extended: Sends extended community attributes.
standard: Sends standard community attributes.

Usage

Use this command to enable the exchange of routing information with a peer router. The chassis supports a maximum of 64 peers per context.

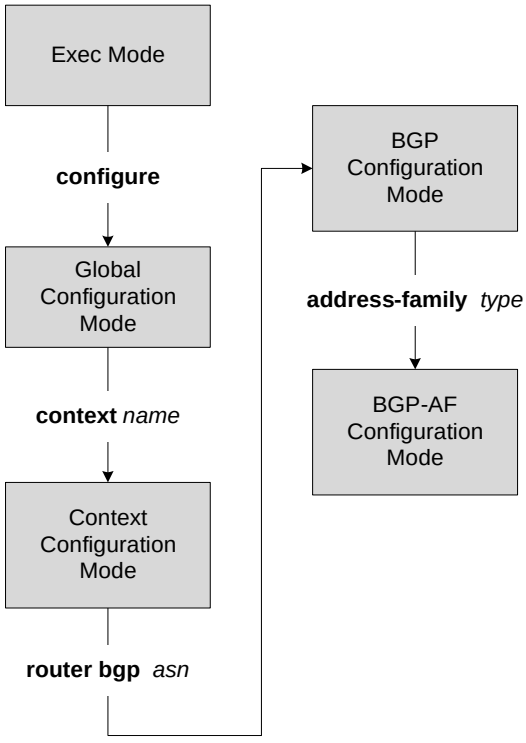
Example

The following command enables the exchange of routing information with the neighbor at IP address *192.168.100.25*:

```
neighbor 192.168.100.25 activate
```

Chapter 36
BGP Address-Family (VRF) Configuration Mode Commands

The Border Gateway Protocol (BGP) Address-Family (VRF) Configuration Mode is used to configure the Virtual Routing and Forwarding address family information.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

neighbor

Configures the Virtual Routing and Forwarding (VRF) address family for BGP routers that interconnect to non-broadcast networks.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] neighbor *ip_address* **{ activate | advertisement-interval** *adv_time* **| default-originate [route-map** *map_name* **] | distribute-list** *dist_list* **{ in | out } | ebgp-multihop [max-hop** *number* **] | filter-list** *filt_list* **{ in | out } | max-prefix** *max_num* **[threshold** *thresh_percent* **] [warning-only] | remote-as** *AS_num* **| remove-private-AS | route-map** *map_name* **{ in | out } | shutdown | srp-activated-soft-clear | timers { [connect-interval** *conn_time* **] | [keepalive-interval** *keep_time* **holdtime-interval** *hold_time* **] } | update-source** *ip_address* **| weight** *value* **}**

no

Delete the specified parameter from the router configuration.

neighbor *ip_address*

Specifies the IP address of the peer router (neighbor) in IPv4 dotted-decimal or IPv6 colon-separated notation.

activate

Enables the exchange of routes with this neighbor.

advertisement-interval *adv_time*

The minimum interval (in seconds) between sending BGP routing updates.
adv_time must be an integer from 0 through 600.
Default: 30

default-originate [route-map *map_name* **]**

Originate default routes to this neighbor
route-map *map_name*: Specifies the route-map that contains the criteria to originate default routes.
map_name must be the name of an existing route-map in the current context.

distribute-list *dist_list* **{in | out}**

Filter updates to and from this neighbor based on a route access list.
Default: No filtering is performed.
dist_list: The name or number of an existing route-access-list.
in: Indicates that incoming advertised routes should be filtered.
out: Indicates that outgoing advertised routes should be filtered.

ebgp-multihop [max-hop *number***]**

Allow external BGP (eBGP) neighbors not on directly connected networks.
max-hop *number*: The maximum number of hops allowed to reach a neighbor. *number* must be an integer from 1 through 255.
Default hop count: 255

filter-list *filt_list* **{ in | out }**

Establish BGP filters based on an AS path access list
filt_list: The name of an existing AS path access list.
in: Indicates that incoming advertised routes will be filtered.
out: Indicates that outgoing advertised routes will be filtered.

max-prefix *max_num* **[threshold** *thresh_percent* **] [warning-only]**

The maximum number of prefixes accepted from this peer. When the maximum is exceeded the neighbor connection is reset.
max_num: Specifies the maximum number of prefixes permitted. This must be an integer from 1 through 4294967295.
Default: No maximum prefix limit.
threshold *thresh_percent*: A percentage value which specifies that when the BGP table is the specified percentage full from this peer warnings are sent to the neighbor. *thresh_percent* must be an integer from 1 through 100.
warning-only: This keyword specifies that only a warning message is sent when the limit is exceeded. The neighbor connection is not reset

remote-as *AS_num*

Specify the AS number of the BGP neighbor.
AS_num: The neighbor's autonomous system number. must be an integer from 1 through 65535.

remove-private-AS

Remove the private AS number from outbound updates.
Default: Do not remove the private AS number.

route-map *map_name* **{ in | out }**

Apply a route map to the neighbor.
map_name: Specifies the route-map apply. *map_name* must be the name of an existing route-map in the current context.
in: Indicates that the route map applies to incoming advertisements.
out: Indicates that the route map applies to outgoing advertisements.

shutdown

Administratively shut down this neighbor. This disables exchanging routes or configuring parameters for this neighbor.

srp-activated-soft-clear

Enables BGP updates when SRP-enabled resources are modified.

timers {[connect-interval *conn_time* **] | [keepalive-interval** *keep_time* **holdtime-interval** *hold_time* **]}**

BGP timers for the specified neighbor.
connect-interval *conn_time*: Specifies the connect timer in seconds. *conn_time* must be an integer from 0 through 65535. The default is 60 seconds.
keepalive-interval *keep_time*: The frequency (in seconds) at which the current BGP router sends keepalive messages to its neighbor. *keep_time* must be an integer from 0 through 65535. The default is 30 seconds.
Holdtime-interval *hold_time*: The interval (in seconds) the router waits for a keepalive message before declaring a neighbor dead. *hold_time* must be an integer from 0 through 65535. The default is 90 seconds.

update-source *ip_address*

use this keyword to bind the specified IP address to the BGP socket that is used to communicate to the peer. *ip_address* is an IPv4 address in dotted-decimal notation.
In most cases you should set the update-source address to the address of the loopback interface in the current context. By doing this, the TCP connection does not go down until there is no route for the loopback address in the peering router.

weight *value*

This command sets the default weight for routes from this neighbor.
value: This must be an integer from 0 through 65535.
Default: 0

Usage

Use this command to set parameters for communication with a specified neighbor. The chassis supports a maximum of 64 peers per context.

Important: A remote AS number must be specified for a neighbor before other parameters can be configured.

Example

The following command specifies that the neighbor at the IP address *192.168.100.25* has an AS number of *2000*:

```
neighbor 192.168.100.25 remote-as 2000
```

The following command allows BGP neighbors that are a maximum of *27* hops away:

```
neighbor 192.168.100.25 ebgp-multihop max-hop 27
```

The following command sets the minimum interval between sending routing updates to 3 minutes (180 seconds):

```
neighbor 192.168.100.25 advertisement-interval 180
```

The following command sets the default weight for all routes from the specified neighbor to *100*:

```
neighbor 192.168.100.25 weight 100
```

redistribute

Redistributes routes into BGP. This means that any routes from another protocol are redistributed to BGP neighbors using the BGP protocol.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] redistribute {connected | ospf | rip | static} [route-map map_name]
```

no

Remove the specified redistribution parameters from the BGP router configuration.

connected

Specifies that connected routes will be redistributed.

ospf

Specifies that Open Shortest Path First (OSPF) routes will be redistributed

rip

Specifies that Routing Information Protocol (RIP) routes will be redistributed. (RIP is not supported at this time.)

static

Specifies that static routes will be redistributed.

route-map *map_name*

Filter routes through the specified route map before redistribution.
map_name specifies the name of the route-map to use and must be specified as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to specify what routes this BGP router should redistribute into BGP.

Example

The following command redistributes OSPF routes after filtering them through the route map named *Map1*:

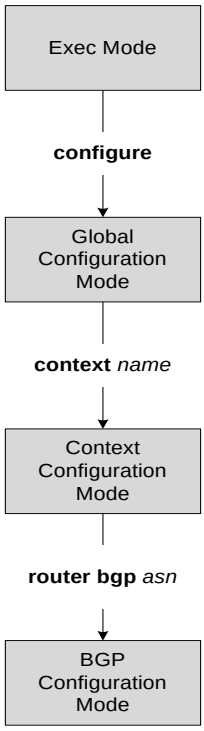
```
redistribute ospf route-map Map1
```

The following command removes the redistribution of OSPF routes from the router's configuration:

```
no redistribute ospf route-map Map1
```

Chapter 37
BGP Configuration Mode Commands

The Border Gateway Protocol (BGP) Configuration Mode is used to configure properties for BGP-4 routing.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

address-family ipv4

Configures the IPv4 Address Family information for the specified BGP Autonomous System (AS) number. Optionally, it also enables the Virtual Routing and Forwarding (VRF) routing information, if specified.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] address-family ipv4 [vrf *vrf_name*]

no

Removes the configured IPv4 address family VRF mode for specific BGP AS number.

address-family ipv4

Enters the BGP Address-Family IPv4 mode to allow entry of IPv4 BGP parameters for the BGP AS number.

Important: The route distinguisher ID must be configured for the VRF name via the **route-distinguisher** command in BGP VRF Configuration mode, before using this keyword.

vrf *vrf_name*

Enables the exchange of VRF routing information. When this keyword is specified with this command, the address family mode changed to VRF address family mode for specific BGP AS number. *vrf_name* is the name of an existing VFR expressed as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the IPv4 or IPv6 BGP address family configuration parameters and optionally enables the exchange of VRF routing information.
Use of the **address-family ipv4** command switches the command mode to BGP Address Family Configuration Mode; the CLI prompt changes to:

```
[context_name>]host_name(config-bgp-af-v4)#
```

Use of **address-family ipv4 vrf** *vrf_name* command switches the command mode to BGP Address Family Configuration Mode; the CLI prompt changes to:

```
[context_name>]host_name(config-bgp-af-vrf)#
```

Example

Use the following command to enter the IPv4 BGP Address-Family configuration mode:

```
address-family ipv4
```

Use following command to enter the IPv4 VRF BGP Address-Family configuration mode for exchange of VRF routing information from VRF *route_vrf1*:

```
address-family ipv4 vrf route_vrf1
```

address-family ipv6

Configures the IPv6 Address Family information for the specified BGP AS number.

Product

All

Privilege

Security Administrator, Administrator

Syntax

address-family ipv6

address-family ipv6

Enters the BGP Address-Family IPv6 mode to allow entry of IPv6 BGP parameters for the BGP AS number.

Usage

Use this command to configure the IPv6 BGP address family configuration parameters for BGP router. Use of **address-family ipv6** command switches the command mode to BGP Address Family Configuration Mode; the CLI prompt changes to:

```
[context_name>]host_name(config-bgp-af-v6)#
```

Example

Use the following command to enter the IPv6 BGP Address-Family configuration mode:

```
address-family ipv6
```

address-family vpnv4

Configures the VPNv4 Address Family information for the specified BGP AS number.

Product

All

Privilege

Security Administrator, Administrator

Syntax

address-family vpnv4

address-family vpnv4

Enters the BGP Address-Family VPNv4 mode to allow entry of VPN BGP parameters for the BGP AS number.

Usage

Use this command to configure the VPNv4 address family configuration parameters for BGP router. This command is also used to switch the command mode to enter the BGP Address Family Configuration Mode. Use of **address-family vpnv4** command switches the command mode to BGP Address Family Configuration Mode; the CLI prompt changes to:

```
[context_name>]host_name(config-bgp-af-vpnv4)#
```

Example

Use the following command to enter the BGP Address-Family configuration mode for VPNv4 address parameters:

```
address-family vpnv4
```

bgp

Defines the BGP-specific parameters regarding graceful restarts.

Product

All

Privilege

Security Administrator, Administrator

Syntax

bgp graceful-restart { restart-time *rest_time* **| stalepath-time** *stale_time* **| update-delay** *delay* **}**

no

Removes the specified administrative distance for the specific route.

graceful-restart restart-time *rest_time*

Specifies the maximum time (in seconds) required for neighbor(s) to gracefully restart. *rest_time* must be an integer from 1 through 3600.

graceful-restart stalepath-time *stale_time*

Specifies the maximum time (in seconds) to retain stale paths from restarting neighbor(s). *stale_time* must be an integer from 1 through 3600.

graceful-restart update-delay *rest_time*

Specifies the maximum time (in seconds) to defer initial route-selection. *update-delay* must be an integer from 1 through 3600.

Usage

Use this command to set BGP-specific parameters regarding graceful restarts.

Example

Use the following command to retain stale paths from restarting neighbor(s) for *100* seconds:

```
bgp graceful-restart stalepath-time 100
```

distance

Defines the administrative distance for routes. The administrative distance is the default priority for a specific route or type route.

Product

All

Privilege

Security Administrator, Administrator

Syntax

distance { admin *distance* **prefix** *prefix_addr* **[route-access-list** *list_name* **] | bgp external** *ebgp_dist* **internal** *ibgp_dist* **local** *local_dist* **}**

no distance { admin *distance* **prefix** *prefix_addr* **[route-access-list** *list_name* **] | bgp [external** *ebgp_dist* **internal** *ibgp_dist* **local** *local_dist* **] }**

no

Removes the specified administrative distance for the specific route.

distance admin *distance* **prefix** *prefix_addr* **[route-access-list** *list_name* **]**

Sets the administrative distance to a specified value for routes with a specific IP prefix. If you also specify a route access list, the IP prefix must match the rules of that access list.
admin *distance*: Specifies the administrative distance that you want to apply to the IP prefix. *distance* must be an integer from 1 through 254.
prefix *prefix_addr*: Specifies the IP prefix of routes that should have the admin distance applied. *prefix_addr* must be an IPv4 address in dotted-decimal notation and the number of subnet bits, representing the subnet mask in CIDR shorthand (for example, 10.1.1.1/24).
route-access-list *list_name*: Defines the name of a route access list that defines for which routes the administrative distance should be set.

distance bgp external *ebgp_dist* **internal** *ibgp_dist* **local** *local_dist*

Sets the administrative distance for external (eBGP), internal (iBGP) and local routes.
external *ebgp_dist*: Sets the administrative distance for eBGP routes. *ebgp_dist* must be an integer from 1 through 254.
internal *ibgp_dist*: Sets the administrative distance for iBGP routes. *ibgp_dist* must be an integer from 1 through 254.
local *local_dist*: Sets the administrative distance for local routes. *local_dist* must be an integer from 1 through 254.

Usage

Use this command to set the administrative distance for specific routes to values that you specify. These values are only applied to the current router.

Example

Use the following command to set the administrative distance to *100* for all routes that have an IP prefix of *192.168.0.0* with a netmask of *16* and are specified in a remote access list named *racl1*:

```
distance admin 100 prefix 192.168.0.0/16 route-access-list rac11
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

enforce-first-as

Enforces the first Autonomous System (AS) for Exterior Border Gateway Protocol (eBGP) routes. An AS is a connected group of one or more Internet Protocol prefixes run by one or more network operators which has a single and clearly defined routing policy (RFC 1930).

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] enforce-first-as
```

no

Disables the enforcement of the first AS for Exterior Border Gateway Protocol (eBGP) routes.

enforce-first-as

Enables the enforcement of the first AS for Exterior Border Gateway Protocol (eBGP) routes.

Usage

Use this command to enforce the use of the first AS for EBGP routes.

Example

Use the following command to enable this functionality:

```
enforce-first-as
```

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

ip vrf

Adds a preconfigured IP VRF context instance to the BGP ASN and configures the BGP attributes and related parameters to the VRF. This command also switches the command mode to BGP VRF Configuration mode.

Product All

Privilege

Security Administrator, Administrator

Syntax

[no] ip vrf *vrf_name*

no

Removes an associated IP VRF from specified BGP AS number and other configured parameters.

vrf_name

Specifies the IP VRF context configured in the Context configuration mode and to be associated with a BGP AS number. *vrf_name* must be an alphanumeric string of 1 through 79 characters identifying an existing instance.

Usage

Use this command to associate the specified IP VRF context instance to the BGP AS number and configures the BGP attributes and related parameters to the VRF. This command also switches the command mode to BGP VRF Configuration mode.
This command switches the command mode to BGP IP VRF Configuration Mode; the CLI prompt changes to:

```
[context_name>]host_name(config-bgp-vrf)#
```

Example

The following command associates the pre-defined VRF context instance *router_mpls* to this BGP AS number:

```
ip vrf router_mpls
```

maximum-paths

Enables forwarding packets over multiple paths and specifies the maximum number of external BGP (eBGP) or internal BGP (iBGP) paths between neighbors.

Product All

Privilege

Security Administrator, Administrator

Syntax

maximum-paths { ebgp *max_num* **| ibgp** *max_num* **}**

[no] maximum-paths { ebgp | ibgp }

no

Disables forwarding packets over multiple eBGP or iBGP paths between neighbors.

ebgp *max_num*

Enables forwarding packets over multiple eBGP paths between neighbors and specifies the maximum number of eBGP paths. *max_num* must be an integer from 1 through 10.

ibgp *max_num*

Enables forwarding packets over multiple iBGP paths between neighbors and specifies the maximum number of iBGP paths. *max_num* must be an integer from 1 through 10.

Usage

Use this command to enable or disable forwarding packets over multiple paths between neighbors and specify the maximum number of EBGP or IBGP paths.

Example

To enable forwarding packets over multiple paths and set the maximum number of EBGP paths to *10*, enter the following command:

```
maximum-paths ebgp 10
```

To disable forwarding packets over multiple EBGP paths, enter the following command:

```
no maximum-paths ebgp
```

neighbor

Configures BGP routers that interconnect to non-broadcast networks. Note that a remote AS number must be specified for a neighbor before other parameters can be configured.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] neighbor *ip_address* **{ activate | advertisement-interval** *adv_time* **| capability graceful-restart | default-originate [route-map** *map_name* **] | distribute-list** *dist_list* **{ in | out } | ebgp-multihop [max-hop** *number* **] | encrypted password** *encrypted password* **| fall-over bfd [multihop] | filter-list** *filt_list* **{ in | out } | max-prefix** *max_num* **[threshold** *thresh_percent* **] [warning-only] | next-hop-self | password** *password* **| remote-as** *AS_num* **| remove-private-AS | restart-time** *rest_time* **| route-map** *map_name* **{ in | out } | send-community { both | extended | standard } | shutdown | srp-activated-soft-clear | timers { [connect-interval** *conn_time* **] | [keepalive-interval** *keep_time* **holdtime-interval** *hold_time* **] } | update-source** *ip_address* **| weight** *value* **}**

no

Delete the specified parameter from the router configuration.

neighbor *ip_address*

Specifies the IP address of a BGP neighbor. *ip_address* must be in IPv4 dotted-decimal or IPV6 colon-separated notation.

activate

Enable the exchange of routes with this neighbor.

advertisement-interval *adv_time*

The minimum interval (in seconds) between sending BGP routing updates. *adv_time* must be an integer from 0 through 600. Default: 30

capability graceful-restart

Configures BGP graceful restart attributes.

default-originate [route-map *map_name* **]**

Enables the origination of default routes to this neighbor
route-map *map_name*: Specifies the route-map that contains the criteria to originate default routes. *map_name* must be the name of an existing route-map in the current context.

distribute-list *dist_list* **{ in | out }**

Filters updates to and from this neighbor based on a route access list. *dist_list*: The name or number of an existing route-access-list. Default: No filtering is performed.

in: Indicates that incoming advertised routes should be filtered.
out: Indicates that outgoing advertised routes should be filtered.

---

ebgp-multihop [max-hop *number* **]**

Allows EBGP neighbors that are not on directly connected networks.
[max-hop] *number*: Specifies the maximum number of hops allowed to reach a neighbor. *number* must be an integer from 1 through 255. Default hop count: 255

---

encrypted password *encrypted password*

Specifies an encrypted password that is used only inside configuration files. This should be an alphanumeric string of 1 through 523 characters.

---

fall-over bfd [multihop]

Enables Bidirectional Fwarding Detection (BFD) multihop support for fallover.
This command adds or modifies a session in BFD for the BGP peer. If there is an existing session in BFD (same source-address/destination address), BGP protocol will be added to the list of clients for the BFD session. BGP will then be notified when there is a change in the BFD session state.
If there is no such BFD session, a new session is added in BFD. For MH-BFD, the session inherits the parameters including min-tx, min-rx, multiplier and authentication from the multihop-peer configuration in BFD by matching the destination address. If the parameters (interval) are not configured in BFD, then the BFD session will be in Admin-down state.
BGP adds a session in BFD only when the BGP peer is Established state. If there is a state transition in bgp where the peer is no longer in established state, then the bfd session is deleted. It will be added again, once the peer comes back to Established state.

---

filter-list *filt_list* **{ in | out }**

Establishes BGP filters based on an AS path access list. **filt_list** is the name of an existing AS path access list.
in: Indicates that incoming advertised routes will be filtered.
out: Indicates that outgoing advertised routes will be filtered.

---

max-prefix *max_num* **[threshold** *thresh_percent* **] [warning-only]**

The maximum number of prefixes accepted from this peer. When the maximum is exceeded the neighbor connection is reset.
Default: No maximum prefix limit.
max_num: Specifies the maximum number of prefixes permitted. This must be an integer from 1 through 4294967295.
[threshold *thresh_percent* **]**: Specifies a percentage value of when the BGP table is full. When this value is reached, peer warnings are sent to the neighbor and the neighbor connection is reset.
thresh_percent must be an integer from 1 through 100.
[warning-only]: Specifies that only a warning message is sent when the limit is exceeded. The neighbor connection is not reset

---

next-hop-self

Disables the next hop calculation for this neighbor.

password *password*

Specifies a password that is only used inside configuration files. This should be an alphanumeric string of 1 through 24 characters.

remote-as *AS_num*

Specify the AS number of the BGP neighbor.
AS_num: Specifies the neighbor's AS number as an integer from 1 through 65535.

remove-private-AS

Removes the private AS number from outbound updates. Default: Do not remove the private AS number.

restart-time *rest_time*

Specifies the maximum time (in seconds) required for a neighbor to restart. *rest_time* must be an integer between 1 and 3600.

route-map *map_name* **{ in | out }**

Applies a route map to the neighbor. *map_name*i s the name of an existing route-map in the current context.
in: Indicates that the route map applies to incoming advertisements.
out: Indicates that the route map applies to outgoing advertisements.

send-community { both | extended | standard }

Sends the community attributes to a peer router (neighbor).
both: Sends extended and standard community attributes.
extended: Sends extended community attributes.
standard: Sends standard community attributes.

shutdown

Administratively shuts down this neighbor. This disables exchanging routes or configuring parameters for this neighbor.

srp-activated-soft-clear

Enables BGP updates when Service Redundancy Protocol SRP-enabled resources are modified.

timers {[connect-interval *conn_time* **] | [keepalive-interval** *keep_time* **holdtime-interval** *hold_time* **]}**

Specifies BGP timers for this neighbor.
connect-interval *conn_time*: Specifies the connect timer in seconds. *conn_time* must be an integer from 0 through 65535. The default is 60 seconds.
keepalive-interval *keep_time*: The frequency (in seconds) at which the current BGP router sends keepalive messages to its neighbor. *keep_time* must be an integer from 0 through 65535. The default is 30 seconds.
Holdtime-interval *hold_time*: The interval (in seconds) the router waits for a keepalive message before declaring a neighbor dead. *hold_time* must be an integer from 0 through 65535. The default is 90 seconds.

update-source *ip_address*

Binds the specified IP address to the BGP socket that is used to communicate to the peer. *ip_address* is an IPv4 address in dotted-decimal notation.

In most cases you should set the update-source address to the address of the loopback interface in the current context. By doing this, the TCP connection does not go down until there is no route for the loopback address in the peering router.

weight *value*

Sets the default weight for routes from this neighbor. *value* must be an integer from 0 through 65535. Default: 0

Usage

Use this command to set parameters for communication with a specified neighbor. The chassis supports a maximum of 64 peers per context.

Example

The following command specifies that the neighbor at the IP address *192.168.100.25* has an AS number of *2000*:

```
neighbor 192.168.100.25 remote-as 2000
```

The following command allows BGP neighbors that are a maximum of *27* hops away:

```
neighbor 192.168.100.25 ebgp-multihop max-hop 27
```

The following command sets the minimum interval between sending routing updates to 3 minutes (180 seconds):

```
neighbor 192.168.100.25 advertisement-interval 180
```

The following command sets the default weight for all routes from the specified neighbor to *100*:

```
neighbor 192.168.100.25 weight 100
```

network

Specifies a network to announce via BGP.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] network *ip_address*/*mask* **[route-map** *map_name* **]**

no

Delete the specified network from the configuration for the BGP router.

ip_address/*mask*

Specifies the IP address and netmask bits for the network to announce via BGP. *ip_address* is a network IPv4 address in dotted-decimal notation and *mask* is the number of subnet bits, representing a subnet mask in CIDR shorthand. These must be entered in the dotted-decimal notation/subnet bits format (for example, 10.1.1.1/24).

[route-map *map_name* **]**

Filter routes through the specified route map before announcing the network. *map_name* is the name of the route-map to use specified as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to specify a network to announce via BGP.

Example

The following command announces the network *192.168.0.0* with a netmask of *16* via BGP:

```
network 192.168.0.0/16
```

The following command removes the network from the BGP router configuration:

```
no network 192.168.0.0/16
```

redistribute

Redistributes routes via BGP from another protocol to BGP neighbors.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] redistribute { connected | ospf | rip | static } [route-map *map_name* **]**

no

Remove the specified redistribution parameters from the BGP router configuration.

redistribute connected

Specifies that connected routes will be redistributed.

redistribute ospf

Specifies that Open Shortest Path First (OSPF) routes will be redistributed

redistribute rip

Specifies that Routing Information Protocol (RIP) routes will be redistributed. (RIP is not supported at this time.)

redistribute static

Specifies that static routes will be redistributed.

[route-map *map_name* **]**

Filter routes through the specified route map before redistribution. map_name specifies the name of the route-map to use and must be specified as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to specify what routes this BGP router should redistribute into BGP.

Example

The following command redistributes OSPF routes after filtering them through the route map named *Map1*:

```
redistribute ospf route-map Map1
```

The following command removes the redistribution of OSPF routes from the router's configuration:

```
no redistribute ospf route-map map1
```

router-id

Overrides the configured router identifier and causes BGP peers to reset.

Product

All

Privilege

Security Administrator, Administrator

Syntax

router-id *ip_address*

no router-id [*ip_address* **]**

no

Remove the specified router ID from the router's configuration and use the default router ID.

router-id *ip_address*

Specifies the IP address to use as the BGP router ID as an IPv4 address in dotted-decimal notation.

Usage

Use this command to configure a specific router ID that overrides the default.

Example

The following command sets the router ID to *192.168.100.25*:

```
router-id 192.168.100.25
```

scan-time

Configures the BGP background scanner interval. BGP monitors the next hop of the installed routes to verify next-hop reachability and to select, install, and validate the BGP best path. By default, the BGP scanner polls the Routing Information Base (RIB) for this information every 60 seconds. During the 60-second time period between scan cycles, Interior Gateway Protocol (IGP) instabilities or other network failures can cause temporarily black holes and routing loops.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] scan-time *time*

no

Remove the user specified scan time from the router's configuration. The scan time is reset to the default value.

scan-time *time*

Specifies the amount of time (in seconds) to wait between background scans to determine next-hop validity. *time* must be an integer from 5 through 60. Default: 60

Usage

Use this command to set the background scanner interval for the BGP router.

Example

The following command sets the background scanner interval to *30* seconds:

```
scan-time 30
```

timers

Configures BGP routing timers.

Product

All

Privilege

Security Administrator, Administrator

Syntax

timers bgp keepalive-interval *interval* **holdtime-interval** *time* **[min-peer-holdtime-interval** *time* **]**

no

Remove the user specified timer values from the router's configuration. The timer values are reset to the default values.

timers bgp keepalive-interval *interval* **holdtime-interval** *time*

keepalive-interval *interval*: Specifies the interval (in seconds) to wait between sending keepalive packets as an integer from 0 through 65535. Default: 30
holdtime-interval *time*: Specifies the interval (in seconds) after which the neighbor is considered dead if keepalive messages are not received as an integer from 0 through 65535.

[min-peer-holdtime-interval *time* **]**

Specifies the interval (in seconds) that is the minimum acceptable hold time from a neighbor as an integer from 0 through 65535. The default is 0 so that there is no restriction on the hold time received in an OPEN message from the peer.

Usage

Use this command to configure the how long to wait between sending keepalive packets and how long to wait for a keepalive before considering a a neighbor dead.

Example

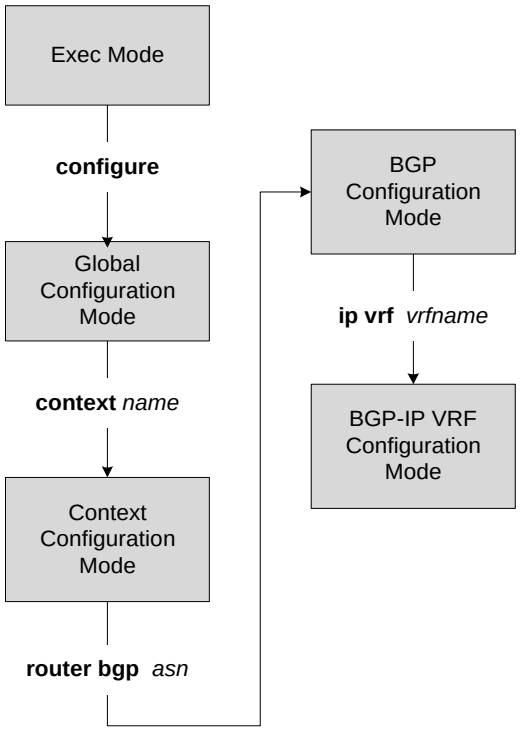
The following command sets the keepalive interval to 2 minutes (120 seconds) and the holdtime interval to 3 minutes (180 seconds):

```
timers bgp keepalive-interval 120 holdtime-interval 180 min-peer-
holdtime-interval 0
```

Chapter 38
BGP IP VRF Configuration Mode Commands

The Border Gateway Protocol (BGP) IP VRF (Virtual Routing and Forwarding) Configuration Mode is used to configure properties for BGP-4 routing.

Important: The VRF must have been preconfigured using the **`ip vrf`** command in the Context Configuration mode before you can enter this configuration mode.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

route-distinguisher

Assigns a route distinguisher (RD) for the VRF that helps identify a VPN in a provider's network and allows for overlapping IP space. The route distinguisher must be a unique value on the router for each VRF.

Product

All

Privilege

Security Administrator, Administrator

Syntax

route-distinguisher { *as_value* | *ip_address* } *rd_value*

route-distinguisher *as_value rd_value*

Identifies the target VRF by an autonomous system (AS) number. *ASN value* is a 16-bit ASN expressed as an integer from 0 through 65535.

route-distinguisher *ip_address rd_value*

Identifies the target VRF by its IP address. *ip_address* is entered using IPv4 dotted-decimal notation.

rd_value

rd_value is a unique route distinguisher identifier and must be an integer from 0 through 4294967295.

Usage

Use this command to assign a router distinguisher (RD) for the IP VRF. The combination of AS number or IP address and RD value must be unique for every VRF configured. The RD is added to the beginning of the pool addresses to change them into globally unique VPN-IPv4 prefixes.
If the RD is not configured for a VRF, user cannot enter into the BGP Address-Family mode for that VRF to configure the neighbors or other related BGP commands.
An RD assigned to a VRF cannot be changed until the existing VRF is deleted or removed and reconfigured.

Example

The following command assigns a router distinguisher *12345* to VRF with AS number *300*:

```
route-distingusher 300 12345
```

The following command assigns a router distinguisher *12345* to VRF with IP address *10.5.3.4*:

```
route-distingusher 10.5.3.4 12345
```

route-target

Adds an export and/or import list of extended route target communities to the VRF. BGP uses an extended-community attribute, the route target, to filter appropriate VPN routes into the correct VRFs. You configure the export list on the VRF to specify export route targets. When BGP advertises a route from this VRF's forwarding table, it associates the list of export route targets with the route and includes this attribute in the update message that advertises the route. You also configure a route-target import list on each VRF to specify import route targets.

Product

All

Privilege

Security Administrator, Administrator

Syntax

route-target { both | import | export } { *as_value* **|** *ip_address* **}** *rt_value*

route-target both

Creates a list of import and export route targets for the VRF with the same parameters. The list contains an AS number or IP address along with a route target (RT) value.

route-target import

Creates a list of import RTs for the VRF with the same parameters. The list contains an AS number or IP address along with an RT value.

route-target export

Creates a list of export RTs for the VRF with the same parameters. The list contains an AS number or IP address along with an RT value.

as_value

Specifies a 16-bit autonomous-system (AS) number expressed as an integer from 0 through 65535.

ip_address

Specifies an IP address in IPv4 dotted-decimal notation.

rt_value

Specifies a unique RT identifier as an integer from 0 through 4294967295.

Usage

Use this command to create the list of export and/or import route target extended communities for VRF.
A maximm of 5 route targets can be defined with this command up to release 9.0.
A maximm of 10 route targets can be defined with this command from release 10.0 onward.

Important: This command must be executed for each route target extended community.

Example

The following command creates an export list of route target extended community *12345* for VRF with AS number *300*:

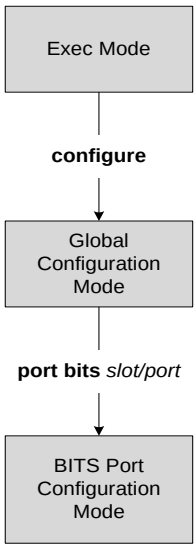
```
route-target export 300 12345
```

The following command creates an export list of route target extended community *12345* for VRF with IP address *192.168.1.2*:

```
route-target export 192.168.1.2 12345
```

Chapter 39
BITS Port Configuration Mode Commands

The Building Integrated Timing Supply (BITS) port configuration mode provides the commands to configure the BITS ports on the SPIO and optionally to configure the transmit timing source.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

default

Restores the port's default speed and communication mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
default { mode | preferred slot }
```

mode

Default: none
Sets the default for the ports framing mode.

preferred slot

Default: non-revertive
Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a port switch command to return service to the original port.

Usage

Restores port-level parameters to their default values.

Example

Use the following command to remove any setting for this port's framing mode:

```
default mode
```

description

Defines descriptive text that provides useful information about the port.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

description *text*

no description

no

Erases the port's description from the configuration file.

text

text must be a string of 1 to 79 alphanumeric characters with no spaces or a string within double quotes that includes printable characters. The description is case-sensitive.

Usage

Set the description to provide helpful information, for example the port's primary function, services, end users. Define any information, the only limit is the number of characters.

Example

Use the following command to set a sample port description in the configuration file:

description *samplePortDescriptiveText*

Use the following command to set a more readable description:

description *"This is a sample description"*

end

Exits the BITS port configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the BITS port configuration mode and returns to the Global configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the Global configuration mode.

mode

Configures the framing mode for the port.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mode { e1 | t1 } framing *type*

e1 | t1

e1 selects the SDH E1 framing mode.
t1 selects the SONET T1 framing mode.

framing *type*

basic: Selects the Frame Alignment Signal (FAS) used with E1.
crcmf: Selects the Multiframe with CRC (FAS+CRC) used with E1.
esf: Selects the extended superframe format used with T1.
sf: Selects the superframe format (D4) used with T1.

Usage

Set the ports framing mode parameters.

Example

Configure the port to support E1 with crcmf framing.

```
mode e1 framing crcmf
```

preferred slot

Identifies which card in a chassis should assume revertive (redundancy auto-recovery) functionality should the slot/port being configured go down. There are only two SPIO, one in slot 24 and the other in slot 25.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

preferred slot *slot#*

[default | no] preferred slot

default

Default: non-revertive operation.

no

Disables revertive, or auto-recovery, operation for the port.

slot#

Identifies the physical slot in the chassis where the SPIO is installed.

Usage

This command enables or disables revertive port redundancy. So after a port failover, when the original port is restored to service (i.e. link up) the system will return service to that port automatically.
Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a **port switch** to command to return service to the original port.

Example

Use this command to set the ports on the card in slot 25 as “preferred” for port redundancy:

preferred slot *25*

recover

Configure line-timing so the SPIO recovers the transmit timing source from an external source via one of the line cards in the chassis. The recovered clock is then distributed for use to all line cards in the chassis.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

recover { line1 *slot#* **| line2** *slot #* **}**

no recover { line1 | line2 }

no

Deletes the identified line-timing source definition from the configuration.

line1 *slot#*

Sets first priority for line-timing clock recovered from the line card in the specified slot.
slot#: a number between 1 and 48.

line2 *slot#*

Sets second priority for line-timing clock recovered from the line card in the specified slot.
slot#: a number between 1 and 48. Can not be the same slot number entered for **line1**.

Usage

Define which line-timing source has priority.

Example

Configure the line card in slot 19 as the preferred source for line-timing.

```
recover line1 19
```

shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, this command with the **no** keyword enables the port and BITS -timing as a transmit timing source.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] shutdown
```

no

Enables the port's administrative state. When omitted the card is shutdown (removed from service).

Usage

Shut down a port prior to re-cabling and/or other maintenance activities.
This command with the **no** keyword is required to bring a port into service.

Example

Use the following command to enable the port for service:

```
no shutdown
```

snmp trap link-status

Enables/disables the generation and sending of an SNMP (notification) trap when the port experiences a change of state (up or down).

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] snmp trap link-status
```

no

Disables the sending of traps for link-status changes.

Usage

Enable the sending of link-status change traps if there is a monitoring facility that can use the information or if there are troubleshooting activities in progress.

Example

Use this command to enable sending of link-status SNMP traps:

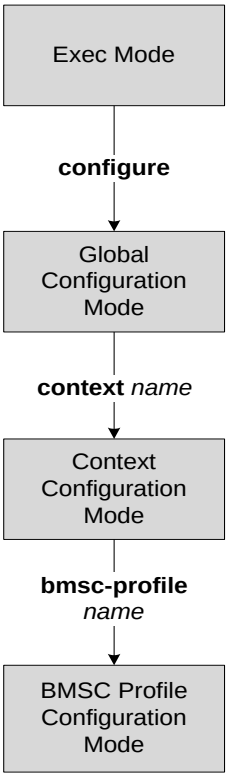
```
snmp trap link-status
```

Use this command to disable sending of link-status SNMP traps:

```
no snmp trap link-status
```

Chapter 40
BMSC Profile Configuration Mode Commands

The BMSC Profile Configuration Mode is used to configure Broadcast Multicast Service Center profiles for Multimedia Broadcast Multicast Service (MBMS) applications. The mode is accessed by entering the **`bmsc-profile`** command from the Context Configuration Mode.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Returns the CLI prompt to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

Example

```
end
```

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Return to the previous or parent mode.

Example

exit

gmb diameter dictionary

This command specifies the Diameter dictionary for the Gmb interface in the BMSC profile of an MBMS user service.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
gmb diameter dictionary { custom1 | custom10 | custom2 | custom3 | custom4 | custom5 |
custom6 | custom7 | custom8 | custom9 | standard }

default gmb diameter dictionary
```

custom1 ... custom10

Custom-defined Diameter dictionary. Specific to customer requirement.

standard

Default: Enabled
Specifies the standard Gmb Diameter dictionary conforming to 3GPP TS 29.061 (Rel. 7).

default

Sets the Diameter dictionary to standard.

Usage

Use this command to select the Gmb Diameter dictionary in BM-SC profile of MBMS user service.

Example

The following command sets the Gmb Diameter dictionary to TS 29.061 (Rel. 7) specific:

```
gmb diameter dictionary standard
```

gmb diameter endpoint

This command specifies the Diameter endpoint name for the Gmb interface in the BMSC profile of an MBMS user service.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

gmb diameter endpoint *endpoint_name*

no gmb diameter endpoint

no

Removes the previously configured Diameter endpoint name for the Gmb interface in the BMSC profile of an MBMS user service.

endpoint_name

Specifies the Diameter endpoint name for Gmb interface. This must be present in all Diameter messages and is the endpoint that originates the Diameter message.
endpoint_name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to create a Gmb Diameter endpoint for a BMSC profile.

Example

The following command creates a Diameter endpoint named *test1* in the BMSC profile of an MBMS user service:

```
gmb diameter endpoint test1
```

gmb diameter peer-select

This command specifies the peer ids of BM-C Diameter primary and secondary host in the BMSC profile for an MBMS user service.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

gmb diameter peer-select peer *peer_name* **[realm** *realm_name* **] [secondary-peer** *sec_peer_name* **[realm** *sec_realm_name* **]]**

gmb diameter peer-select

no

Removes the previously configured BM-C Diameter peer ids configured in the BMSC profile of an MBMS user service.

peer *peer_name*

Specifies the primary diameter host id for BMSC in this BMSC profile for MBMS user service. This is a unique name that is specified for the primary peer.
peer_name must be an alphanumeric string of 1 through 127 characters including punctuation marks.

realm *realm_name*

Specifies the realm or domain for the Gmb Diameter peer. The realm may typically be a company or service name.
realm_name must be an alphanumeric string of 1 to 127 characters including punctuation marks.

secondary-peer *sec_peer_name*

Specifies a back-up host that is used for fail-over processing. When the route-table does not find an AVAILABLE route, the secondary host performs fail-over processing.
sec_peer_name must be an alphanumeric string of 1 through 127 characters including punctuation marks.

realm *sec_realm_name*

Specifies the realm or domain for the Gmb Diameter secondary host. The realm may typically be a company or service name.
sec_realm_name must be an alphanumeric string of 1 through 127 characters including punctuation marks.

Usage

Use this command to select a BMSC Diameter peer and realm in this BMSC profile for MBMS user service.

Example

The following command selects a Gmb Diameter peer named *test1* and a realm of *companyx*:

```
gmb diameter peer-select peer test1 realm companyx
```

gmb user-data

This command configures the parameters in this BMSC profile for user data for MBMS user service.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

gmb user-data { mode-preference { multicast | unicast } | unicast-self-address *self_ip_address* **}**

default gmb user-data mode-preference

no gmb user-data unicast-self-address

no

Removes the configured self address of GGSN for unicast in the BMSC profile for user data of MBMS user service.

defualt

Sets the user data mode to unicast in the BMSC profile for user data of MBMS user service.

mode-preference { multicast | unicast }

Default: unicast
Specifies the preferred mode of GGSN for receiving MBMS user service data.
multicast: specifies the preferred mode as multicast for MBMS user service.

Important: Note that this **multicast** keyword is not supported in this release.

unicast: specifies the preferred mode as unicast for MBMS user service.

unicast-self-address *self_ip_address*

Specifies the GGSN's IP address for BMSC to use as the outer destination address for the IP-in-IP tunnel to send multicast data, if the configured preferred data mode is unicast.
self_ip_address must be the IPv4 address in dotted-decimal notation.
This command must be configured if GGSN's user-data mode-preference is Unicast.

Usage

Use this command to configure user data mode and other parameters in the BMSC profile for user data of MBMS user service.
GGSN can receive multicast data from BMSC in one of two modes - Multicast or Unicast. In Unicast mode, BM-SC tunnels the multicast data to the GGSN in an IP-in-IP tunnel instead of direct multicast. This command with the **mode-preference** keyword configures the GGSN's preferred mode for receiving multicast data.

Important: Both GGSN and BMSC must support the Unicast mode of multicast data transfer. If any GGSN or BMSC does not support Multicast mode, BMSC will transfer multicast data using Unicast mode only.

Use the **unicast-self-address** keyword to configure the GGSN's IP address which the BMSC should use as the outer destination address for the IP-in-IP tunnel to send multicast data, if the selected user data mode to receive multicast data is Unicast.

Example

The following command sets the MBMS data transfer mode to unicast:

```
default gmb user-data mode-preference
```

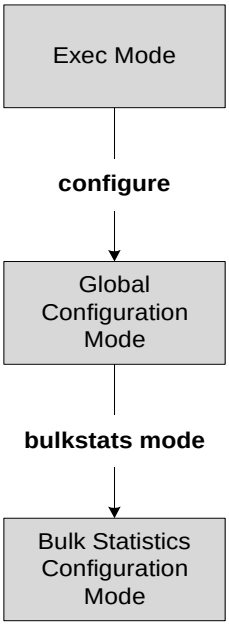
Chapter 41
Bulk Statistics File Configuration Mode Commands

This section describes a bulk statistic “file” under which to group the bulk statistic configuration. The Bulk Statistics File Configuration mode supports the configuration of “files” used for organizing bulk statistics schema, delivery options, and receiver information.

Because multiple “files” can be configured, this functionality provides greater flexibility in that it allows you to configure different schemas to go to different receivers. To configure a bulk statistics file, enter the following command:

Important: Use of bulk statistics “files” is optional. However system logically assigns “file 1” to the standard configuration. Therefore, if you wish to configure bulk statistics “files” at a later time, “file 1” can be used.

Caution: If the Web Element Manager application is used to collect and process (XML parsing, graphing, etc.) bulk statistics data, “file 1” is used by the Web Element Manager’s default bulk statistics collection information and schemas. To avoid errors in processing by the Web Element Manager, do not configure “file 1" via the CLI. However, it is possible to configure files 1 through 4 using the system’s CLI, regardless of whether or not the Web Element Manager is configured as a receiver. In this case, the bulk statistics data is written to the server but not processed by the Web Element Manager application.



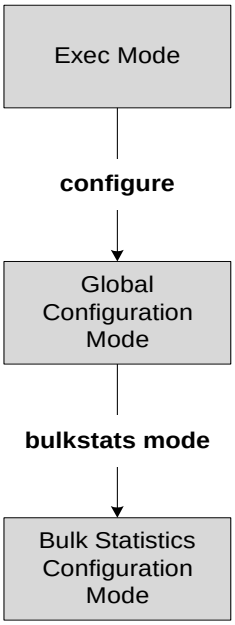
Important: The commands in this configuration mode are identical to the same commands in the “Bulk Statistics Configuration Mode Commands” chapter.

Chapter 42
Bulk Statistics Configuration Mode Commands

The Bulk Statistics Configuration Mode is used to manage the options for the collection, formatting and delivery of system statistics to remote nodes.

Refer to the *Common Syntax Options* section in this chapter for information about formatting the output of bulk statistics.

Important: Unless otherwise indicated, all statistics are counters. For statistics with the Int32 data type, the roll-over to zero limit is 4,294,967,295. For statistics with the Int64 data type, the roll-over to zero limit is 18,446,744,073,709,551,615.



Overview

Schema Format String Syntax

The following defines common syntax block options. These options appear in similar commands and are detailed here for easy reference.

The schema format string is used to define the structure of generated bulk statistics data. The string may contain static text, dynamic content, and bulk statistic variables, or any combination.

Static text includes any ASCII characters that are of a fixed value. Static text may also include control characters by using Escape character sequences. Supported Escape character shortcuts are “\n” for new line and “\t” for tab.

Enclosing an alphanumeric string within double quotation marks (“) allows you to include spaces in the string.

Variables within the format string must be enclosed within “% and %”, for example, “%var%”. The actual variables supported are command-dependent and are described in the *Statistics and Counters Reference*.

Common Statistics

For a list of the statistics that are common to all schema, refer to the *Statistics and Counters Reference*.

aal2 schema

Configures the ATM adaptation layer 2 (AAL2) bulk statistics schema within an ATM virtual connection by the HNB-GW.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

aal2 schema *schema_name* **format** *format_string*

no aal2 schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for ATM adaptation layer 2 (AAL2) bulk statistics collection. Multiple AAL2 schemas can be created to further categorize HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple AAL2 schemas, re-issue the **aal2 schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *aal2stats1* that records the number of AAL2 uplink packets transmitted and AAL2 downlink packets received by Access Link Control Application Part (ALCAP) service on HNB-GW:

```
aal2 schema aal2stats1 format "%uplink-pkts-tx%" "%downlink-pkts-rx%"
```

alcap schema

Configures the Access Link Control Application Part (ALCAP) bulk statistics schema for an ALCAP service on an HNB-GW node.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

alcap schema *schema_name* **format** *format_string*

no alcap schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for Access Link Control Application Part (ALCAP) service bulk statistics collection on HNB-GW node. Multiple ALCAP schemas can be created to further categorize at AAL2 channel-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple ALCAP schemas, re-issue the **alcap schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *alcap1stats1* that records the number of AAL2 channels in connecting and connected state on ALCAP service:

```
alcap schema alcaplstats1 format "%num-aal2-channels-in-connecting%"
"%num-aal2-channels-in-connected-state%"
```

apn schema

Configures the Access Point Name (APN) bulk statistics schema.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

apn schema *schema_name* **format** *format_string*

no apn schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for APN bulk statistics collection. Multiple APN schemas can be created to further categorize APN-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple APN schemas, re-issue the **apn schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *apn1stats1* that records the number of sessions currently facilitated by the APN:

```
apn schema apn1stats1 format "%sess-curr%"
```

asngw schema

Configures Access Service Gateway (ASN-GW) bulk statistics schema.

Product

ASN GW

Privilege

Security Administrator, Administrator

Syntax

asngw schema *schema_name* **format** *format_string*

no asngw schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format. as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for ASN-GW bulk statistics collection. Multiple ASN-GW service schemas can be created to further categorize ASN-GW service bulk statistics. All of the schemas are processed at each collection interval. To create multiple ASN-GW service schemas, re-issue the **asngw schema** *schema_name* command using a different schema name.

Example

To create an ASN-GW schema called *asngw_statistics* that specifies a schema format of:

- VPN context name: *vpnname*
- VPN Context Identifier: *vpnid*
- ASN-GW Service name: *servname*
- ASN-GW Service identifier: *servid*
- Peer IP address: *peeripaddr*

Use the following command:

```
asngw schema asngw_statistics format "VPN name: %vpnname%\nVPN ID:
%vpnid%\nASN-GW Service Name: %servname%\nASN-GW Service Identifier:
%servid%\nPeer IP Address: %peeripaddr%"
```

bcmcs schema

Configures Broadcast and Multicast Service (BCMCS) bulk statistics schema.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

bcmcs schema *schema_name* **format** *format_string*

no bcmcs schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for BCMCS bulk statistics collection. Multiple BCMCS schemas can be created to further categorize BCMCS-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple BCMCS schemas, re-issue the **bcmcs schema** *schema_name* command using a different schema name.

Example

The following command creates a schema named *bcmcs1stats1* that records the number of sessions currently facilitated by BCMCS:

```
bcmcs schema bcmcs1stats1 format "%sess-curr%"
```

card schema

Configures card bulk statistics schema. These are statistics for circuit cards installed in the ASR 5x00 chassis.

Product

All

Privilege

Security Administrator, Administrator

Syntax

card schema *schema_name* **format** *format_string*

no card schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for card bulk statistics collection. Multiple card schemas can be created to categorize card-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple card schemas, re-issue the **card schema** *schema_name* command using a different schema name.

Important: Not supported on all platforms

Example

The following command creates a schema called *card1stats1* that records the number of processes for all installed cards:

```
card schema card1stats1 format "%slot%-%numproc%"
```

To create a card-level schema called *cardresourcestats* that specifies a schema format of:

- Chassis slot number: *slot*
- Available Memory: *memtotal* Memory Used (%): *memused*
- Available CPU (%): *cpuidle*

Use the following command:

```
card schema cardresourcestats format "Chassis slot number:
%slot%\nAvailable Memory: %memtotal%\tMemory Used (%):
%memused%\nAvailable CPU (%): %cpuidle%"
```

context schema

Configures context bulk statistics schema.

Product

All

Privilege

Security Administrator, Administrator

Syntax

context schema *schema_name* **format** *format_string*

no context schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema forma as an alphanumeric string of 1 through 3600 characters. For syntax details, see Schema Format String Syntax section.

Important: For the complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for Context bulk statistics collection. Multiple context schemas can be created to categorize context statistics. All of the schemas are processed at each collection interval. To create multiple context schemas, re-issue the **context schema** *schema_name* command using a different schema name.

Example

To create a Firewall context schema called *sfw_context_stats1* that specifies a schema format of:

- Total packets received by firewall: *sfw-total-rxpackets*
- Total packets sent by firewall: *sfw-total-txpackets*
- Total ICMP packets discarded by firewall: *fw-icmp-discardpackets*

Use the following command:

```
context schema sfw_context_stats1 format "Packets received Rx: %sfw-
total-rxpackets%\nPackets Sent Tx:: %sfw-total-txpackets%\nICMP Packets
discarded: %fw-icmp-discardpackets%"
```

cscf schema

Configures Call Session Control Function (CSCF) bulk statistics schema.

Product

SCM

Privilege

Security Administrator, Administrator

Syntax

cscf schema *schema_name* **format** *format_string*

no cscf schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format. as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for CSCF bulk statistics collection. Multiple CSCF-service schemas can be created to categorize CSCF-service bulk statistics. All of the schemas are processed at each collection interval. To create multiple CSCF-service schemas, re-issue the **cscf schema** *schema_name* command using a different schema name.

Example

To create a CSCF schema called *cscf_statistics* that specifies a schema format of:

- Call attempts received: *callattrx*
- Call attempts transmitted: *callatttx*
- Call successes received: *callsuccrx*
- Call successes transmitted: *callsucctx*
- Call failures received: *callfailrx*
- Call failures transmitted: *callfailtx*

Use the following command:

```
cscf schema cscf_statistics format "Call Attempts Rx: %callattrx%\nCall
Attempts Tx: %callatttx%\nCall Successes Rx: %callsuccrx%\nCall Successes
```

```
Tx: %callsucctx%\nCall Failures Rx: %callfailrx%\nCall Failures Tx:
%callfailtx%”
```

cs-network-ranap

Configures the Radio Access Network Application Part (RANAP) bulk statistics schema in a Circuit Switched (CS) network associated with an HNB-GW node.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

cs-network-ranap schema *schema_name* **format** *format_string*

no cs-network-ranap schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for RANAP procedure related bulk statistics collection in a CS network associated with HNB-GW in a Femto UMTS network. Multiple CS Networks RANAP schemas can be created to further categorize at CS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple CS Networks RANAP schemas, re-issue the **cs-network-ranap schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *cs_ranap1stats1* that records the total number of Iu Release Request messages transmitted and total number of Iu Release Command message received by the HNB-GW node:

```
cs-network-ranap schema cs_ranaplstats1 format "%iu-rel-req-tx%" "%iu-rel-cmd-rx%"
```

cs-network-rtp

Configures the Real-Time Transport Protocol (RTP) bulk statistics schema in a Circuit Switched (CS) network associated with an HNB-GW node.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

cs-network-rtp schema *schema_name* **format** *format_string*

no cs-network-rtp schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for RTP procedure related bulk statistics collection in a CS network associated with HNB-GW in a Femto UMTS network. Multiple CS Networks RTP schemas can be created to further categorize at CS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple CS Networks RTP schemas, re-issue the **cs-network-rtp schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *cs_rtp1stats1* that records the total number of RTP Downlink Packets received and RTP Uplink Packets transmitted by HNB-GW node in an associated CS network:

```
cs-network-rtp schema cs_rtplstats1 format "%rtp-uplink-pkts-tx%" "%rtp-downlink-pkts-rx%"
```

dcca schema

Configures Diameter Credit Control Application (DCCA) bulk statistics schema. This command is available only in 9.0 and later releases.

Product

All

Privilege

Security Administrator, Administrator

Syntax

dcca schema *schema_name* **format** *format_string*

no dcca schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for DCCA bulk statistics collection.

default

Restores the system default for the option specified.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
default { limit | receiver mode | remotefile format | sample-interval | transfer-interval
}
```

limit

Restores the memory utilization limit system default: 1000 kilobytes.

receiver mode

Restores the behavior for sending files to the receivers to the default value.
Default: secondary-on-failure

remotefile format

Restores the format of remote bulkstats file names to the default value.
Default: "%date%-%time%"

sample-interval

Restores the system default for the local polling interval for statistic sampling.
Default: 15 minutes

transfer-interval

Restores the system default for the time between transfer of data files to receivers.
Default: 480 minutes

Usage

Restore the default values when troubleshooting the system. Setting values to the system defaults places them in well known states as starting points for monitoring for problems.

Example

```
default limit

default transfer-interval
```

diameter-acct schema

Configures Diameter Accounting bulk statistics schema. This command is available only in 11.0 and later releases.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter-acct schema *schema_name* **format** *format_string*

no diameter-acct schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for Diameter Accounting bulk statistics collection.

diameter-auth schema

Configures Diameter Authentication bulk statistics schema. This command is available only in 11.0 and later releases.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter-auth schema *schema_name* **format** *format_string*

no diameter-auth schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for Diameter Authentication bulk statistics collection.

dlci-util schema

Configures the collection of statistics for the DLCI-Util (DLCI utilization) schema.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

dlci-util schema *dlci_schema_name* **format** *dlci_schema_format*

no dlci-util schema *dlci_schema_name*

no

Removes the specified schema.

dlci_schema_name

Specifies a name for a model collection schema for DLCI utilization statistics. The name must be comprised of an alphanumeric string of 1 to 31 characters.

format *dlci_schema_format*

Specifies the format of the collected DLCI utilization statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages. The format value comprises an alphanumeric string of 1 through 3599 characters. For syntax details, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for the DLCI-Util schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for DLCI-Util bulk statistics collection in the generated stats report files.. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified. Multiple schemas can be created to categorize DLCI-Util bulk statistics. All of the schemas are processed at each collection interval. To create multiple DLCI-Util schemas, re-issue the **dlci-util schema** *dlci_schema_name* command using a different schema name each time.

Example

Include the bulk statistic variable names to create a schema named *dlciutilstats_sgsn1* that specifies collection of statistics (a schema format) for:

- card
- port
- path
- DS1/E1

- DLCI
- DLCI utilization snapshot for received packets
- DLCI utilization for received packets in the last 5 minutes
- DLCI utilization for received packets in the last 15 minutes

Use the following command:

```
gprs schema gprsstats_sgsn1 format "Card: %card%\nPort: %port%\nDLCI in
path: %dlci_util_path%\nDS1/E1: %dlci_util_ds1e1%\nDLCI ID:
%dlci_util_dlci_no%\nCurrent Rx: %dlci_util_dlci_curr_rx%\nRx in 5
minutes: %dlci_util_dlci_5min_rx%\nRx in 15 minutes:
%dlci_util_dlci_15min_rx%\n"
```

dpca schema

Configures Diameter Policy Control Application (DPCA) bulk statistics schema. This command is available only in 9.0 and later releases.

Product

All

Privilege

Security Administrator, Administrator

Syntax

dpca schema *schema_name* **format** *format_string*

no dpca schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for DPCA bulk statistics collection.

ecs schema

Configures Enhanced Charging Service (ECS) bulk statistics schema.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ecs schema *schema_name* **format** *format_string*

no ecs schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for ECS bulk statistics collection. Multiple ECS schemas can be created to categorize ECS bulk statistics. All of the schemas are processed at each collection interval. To create multiple ECS schemas, re-issue the **ecs schema** *schema_name* command using a different schema name.

egtpc schema

Configures the enhanced GTP-C statistics schema for naming conventions of data files.

Product

P-GW, S-GW

Privilege

Administrator

Syntax

egtpc schema *schema_name* **format** *format_string*

no egtpc schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for enhanced GTP-C bulk statistics collection. Multiple eGTP-C service schemas can be created to categorize eGTP-C service bulk statistics. All of the schemas are processed at each collection interval. To create multiple eGTP-C service schemas, re-issue the **egtpc schema** *schema_name* command using a different schema name.

Example

For an eGTP-C-level schema called *egtpcservicestats* that specifies a schema format of:

- Tunnel - Create Session Request Sent: *tun-sent-cresess*
- Tunnel - Create Session Request Received: *tun-recv-cresess*

Use the following command:

```
egtpc schema egtpcservicestats format "Number of GTP Tunnel Requests
Sent: %tun-sent-cresess%\nNumber of GTP Tunnel Requests Received: %tun-
recv-cresess%\n"
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

fa schema

Configures Foreign Agent (FA) bulk statistics schema.

Product

All

Privilege

Security Administrator, Administrator

Syntax

fa schema *schema_name* **format** *format_string*

no fa schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for FA bulk statistics collection. Multiple FA service schemas can be created to categorize FA service bulk statistics. All of the schemas are processed at each collection interval. To create multiple FA service schemas, re-issue the **fa schema** *schema_name* command using a different schema name.

Example

To create a FA-level schema named *faservicestats* that separates the *date*, *time*, and *vpnname* by tabs, enter the following command:

```
fa schema faservicestats format %date%\t%time%\t%vpnname%
```

The schema format appears as follows:

```
date    time    vpnname
```

file

Enters the Bulk Statistics File Configuration mode which supports the configuration of “files” used for grouping bulk statistic configuration information.

Product

All

Privilege

Security Administrator, Administrator

Syntax

`[ no ] file` *`number`*

`no`

Removes a previously configured bulk statistic file.

`number`

Specifies a number for the bulkstatistics file as an integer from 1 through 4. This number is how the file is recognized by the system.

Usage

Bulk statistics “files” are used to group bulk statistic schema, delivery options, and receiver configuration. Because multiple “files” can be configured, this functionality provides greater flexibility in that it allows you to configure different schemas to go to different receivers. A Maximum of four files can be assigned for bulk statistics collection.

Executing this command allows you to enter the Bulk Statistics File Configuration Mode. This mode supports all of the commands from the Bulk Statistics Configuration mode except **`limit, local-directory, sample-interval,`** and **`transfer-interval`**. (these commands are configured globally for all “files”.)

Important: Use of bulk statistics “files” is optional. If you do not wish to configure bulk statistic “files”, you can perform a standard configuration using the commands in the Bulk Statistic Configuration Mode. Note, however, that the system logically assigns “file 1” to the standard configuration. Therefore, if you wish to configure bulk statistics “files” at a later time, “file 1” will already be used.

Caution: If the Web Element Manager application is used to collect and process (XML parsing, graphing, etc.) bulk statistics data, “file 1” is used by the Web Element Manager’s default bulk statistics collection information and schemas. To avoid errors in processing by the Web Element Manager, do not configure "file 1" via the CLI. However, it is possible to configure files 1 through 4 using the system’s CLI, regardless of whether or not the Web Element Manager is configured as a receiver. In this case, the bulk statistics data is written to the server but not processed by the Web Element Manager application.

Example

The following command creates a bulk statistics file numbered 2 and enters the Bulk Statistics File Configuration Mode:

```
file 2
```

fng schema

Configures Femto Network Gateway (FNG) bulk statistics schema.

Product

FNG

Privilege

Security Administrator, Administrator

Syntax

fng schema *schema_name* **format** *format_string*

no fng schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

footer

Configures the footer string placed at the end of the generated bulk statistics data files.

Product

All

Privilege

Security Administrator, Administrator

Syntax

footer format *format_string*

no footer format

no

Clears the footer format string which results in the default file footer being used in generated data files.

format *format_string*

Specifies the footer format string for use in generated data files as an alphanumeric string from 1 through 2047 characters. The format string syntax is described in the Schema Format String Syntax section. Default: "" (an empty footer)
The following variables are supported:

Table 11. footer Command Format String Variables

Variable	Description	Data Type
date	The date that the collection file was created in YYYYMMDD format where YYYY represents the year, MM represents the month and DD represents the day.	String
host	The system hostname that created the file	String
ipaddr	The default management (local context) IP address in ###.###.###.### format. An empty string is inserted if no address is available.	String
sysuptime	The uptime (in seconds) of the system that created the file.	32-bit signed
time	The time that the collection file was created in HHMMSS format where HH represents the hours, MM represents the minutes, and SS represents the seconds.	String

Usage

Define a unique footer in data files which allows for easy identification of which system generated the data file or any other useful information. The use of the variables is suggested so as to allow for a uniform footer across all systems. The hostname variable should be used to identify the source of the data in the footer and all remaining items can be formatted consistently across all chassis.

Example

The following commands define different footer formats:

```
footer format northStreet

footer format "Created on: %date%-%time% by %host%"

no footer format
```

gather-on-standby

Controls whether or not statistics are gathered when a system is in the standby state.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] gather-on-standby
```

no

Does not gather bulk statistics when the system is in the standby state.

default

Resets this command to its default action of gathering bulk statistics when the system is in the standby state.

Usage

Use this command to configure a system to either gather or not gather statistics when the system is in the standby state. This is useful for systems configured for Interchassis Session Recovery (ICSR). See the *System Administration Guide* for more details on this feature.

If a chassis transitions to standby state and it has accumulated but not yet transferred bulk statistics data, the previously accumulated data is transferred at the first opportunity. However, no additional statistics gathering takes place.

Example

The following command disables gathering statistics when the system is in the standby state:

```
no gather-on-standby
```

The following command enables the gathering of statistics when the system is in the standby state:

```
gather-on-standby
```

gprs schema

Configures the collection of statistics for the GPRS schema.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gprs schema *gprs_schema_name* **format** *gprs_schema_format*

no gprs schema *gprs_schema_name*

no

Removes the specified schema.

gprs_schema_name

Specifies a name for a model collection schema for GPRS statistics. The name must be comprised of an alphanumeric string of 1 to 31 characters.

format *gprs_schema_format*

Specifies the format of the collected GPRS statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages. The format value comprises an alphanumeric string of 1 through 3599 characters. For syntax details, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for the GPRS schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for GPRS bulk statistics collection in the generated stats report files.. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple GPRS schemas can be created to categorize GPRS bulk statistics. All of the schemas are processed at each collection interval. To create multiple GPRS schemas, re-issue the **gprs schema** *gprs_schema_name* command using a different schema name each time.

Example

Include the bulk statistic variable names to create a GPRS schema named *gprsstats_sgsn1* that specifies collection of statistics (a schema format) for:

- context name
- GPRS service name
- number of LLC packets dropped

Use the following command:

```
gprs schema gprsstats_sgsn1 format "Context Name: %vpnname%\nGPRS Service
Name: %servname%\nTotal LLC Packets Dropped: %bssgp-total-usr-req-
drop%\n"
```

gtpc schema

Configures GPRS Tunneling Protocol-Control (GTPC) message statistics schema.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

gtpc schema *gtpc_schema_name* **format** *gtpc_schema_format*

no gtpc schema *gtpc_schema_name*

no

Removes the specified schema.

gtpc_schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *gtpc_schema_format*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for GTPC bulk statistics collection. Multiple GTPC schemas can be created to categorize GTPC bulk statistics. All of the schemas are processed at each collection interval. To create multiple GTPC schemas, re-issue the **gtpc schema** *schema_name* command using a different schema name.

Example

To create a GTPC-level schema named *gtpc_stats* that specifies a schema format of:

- Context Name: *vpnname*
- GGSN Service Name: *servname*
- Total PDP Contexts Processed: *setup-total*

Use the following command:

```
gtpc schema gtpc_stats format "Context Name: %vpnname%\nGGSN Service
Name: %servname%\nTotal PDP Contexts Processed: %setup-total%\n"
```

gtpp schema

Configures GPRS Tunneling Protocol-Prime (GTPP) statistics schema.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp schema *gtpp_schema_name* **format** *gtpp_schema_format*

no gtpp schema *gtpp_schema_name*

no

Removes the specified schema.

gtpp_schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *gtpp_schema_format*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for GTPP bulk statistics collection. Multiple GTPP schemas can be created to categorize GTPP bulk statistics. All of the schemas are processed at each collection interval. To create multiple GTPP schemas, re-issue the **gtpp schema** *schema_name* command using a different schema name.

Example

To create a GTPP schema named *gtpp_statistics* that specifies a schema format of:

- Time: *time*
- Total Redirection Requests Received: *redir-rcvd*

Use the following command:

```
gtpp schema gtpp_statistics format "Time: %time%\tTotal Redirection
Requests Received: %redir-rcvd%\n"
```

gtpu schema

Configures GTP-U bulk statistics schema.

Product

GGSN, HNB-GW, P-GW, S-GW

Privilege

Security Administrator, Administrator

Syntax

gtpu schema *schema_name* **format** *format_string*

no gtpu schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the format of the collected GTP-U statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages. The format value comprises an alphanumeric string of 1 through 3599 characters.The format string syntax is described by Schema Format String Syntax .

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for GTP-U bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified. Multiple GTP-U schemas can be created to categorize GTP-U bulk statistics. All of the schemas are processed at each collection interval. To create multiple GTP-U schemas, re-issue the **gtpu schema** *schema_name* command using a different schema name each time.

ha schema

Configures Home Agent (HA) bulk statistics schema.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

ha schema *schema_name* **format** *format_string*

no ha schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format. as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for HA bulk statistics collection. Multiple HA service schemas can be created to categorize HA service bulk statistics. All of the schemas are processed at each collection interval. To create multiple HA service schemas, re-issue the **ha schema** *schema_name* command using a different schema name.

Example

For an HA schema named *haservicestats* that specifies a schema format of:

- Number of HA authentication failures: *reply-haauthfail*
- Number of Mobile Node authentication failures: *reply-mnauthfail*

Use the following command:

```
ha schema haservicestats format "Number of HA authentication failures:
%reply-haauthfail%\nNumber of Mobile Node authentication failures:
%reply-mnauthfail%\n"
```

header

Configures the header string placed at the beginning of the generated bulk statistics data files.

Product

All

Privilege

Security Administrator, Administrator

Syntax

header format *format_string*

no header format

no

Clears the header format string which results in the default file header being used in generated data files.

format *format_string*

Specifies the header format string for use in generated data files as an alphanumeric string of 1 through 2047 characters. The format string syntax is described in the Schema Format String Syntax section. Default: "" (an empty header)
The following variables are supported:

Table 12. header Command Format String Variables

Variable	Description	Data Type
date	The UTC date that the collection file was created in YYYYMMDD format where YYYY represents the year, MM represents the month and DD represents the day.	String
date3	The UTC date that the collection file was created in YYMMDD format where YY represents the year, MM represents the month and DD represents the day.	String
host	The system hostname that created the file	String
ipaddr	The default management (local context) IP address in ###.###.###.### format. An empty string is inserted if no address is available.	String
sysuptime	The uptime (in seconds) of the system that created the file.	32-bit signed
time	The time that the collection file was created in HHMMSS format where HH represents the hours, MM represents the minutes, and SS represents the seconds.	String

Usage

Define a unique header in data files which allows for easy identification as to which system generated the data file or any other useful information.

Using the variables described above allows for a uniform header across all systems. The hostname variable should be used to identify the source of the data in the header and all remaining items can be formatted consistently across all chassis.

Example

The following commands define different header formats:

```
header format northStreet

header format "Created on: %date%-%time% by %host%"

no header format
```

hnbgw-hnbap schema

Configures bulk statistics schema for HNB-Application Part (HNB-AP) message statistics collection in HNB-GW session instance.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

hnbgw-hnbap schema *schema_name* **format** *format_string*

no hnbgw-hnbap schema *schema_name*

no

Removes the configured HNB-AP schema.

schema_name

Specifies a name for the HNB-AP schema to be used as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies a name for HNB-AP schema format followed by schema variables. *format_string* must be an alphanumeric string of 1 through 3599 characters. For syntax details, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

This command defines schemas used for HNB-AP statistics collection. Multiple HNB-AP schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the **hnbgw-hnbap schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *hnbap1stats1* that records the number of registered UEs and registered HNBs along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-hnbap schema hnbap1stats1 format "%vpnname%-%vpnid%-%servname%-
%registered-hnb%-%registered-ue%"
```

To create a schema called *hnbapuestats* that specifies a schema format of:

- Number of UEs with CS and PS Core Network Connections: *ue-with-ps-cs-conn*
- Number of UEs in Idle Condition: *idle-u*e

Use the following command:

```
hnbgw-hnbap schema hnbapuestats format "Number of UEs with CS and PS Core
Network Connections: %ue-with-ps-cs-conn%\nNumber of UEs in Idle
Condition: %idle-ue%"
```

hnbgw-ranap schema

Configures bulk statistics schema for Radio Access Network-Application Part (RANAP) message statistics collection in HNB-GW session instance.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

hnbgw-ranap schema *schema_name* **format** *format_string*

no hnbgw-ranap schema *schema_name*

no

Removes the configured RANAP schema.

schema_name

Specifies a name for the RANAP schema to be used as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies a name for RANAP schema format, to be used, followed by schema variables. *format_string* must be an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

This command defines schemas used for RANAP messaging statistics collection. Multiple RANAP schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the **hnbgw-ranap schem** *schema_name* command using a different schema name.

Example

The following command creates a schema called *ranap1stats1* that records the number of CS-Direct-Transfer messages sent and received on RANAP along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-ranap schema ranap1stats1 format "%vpnname%-%vpnid%-%servname%-%cs-dir-transfer-rx%-%cs-dir-transfer-tx%"
```

To create a schema called *ranappagingstats* that specifies a schema format of:

- Number of paging requests sent on RANAP from CS Core Network Connections: *cs-paging-req-tx*
- Number of paging requests sent on RANAP from PS Core Network Connections: *ps-paging-req-tx*

Use the following command:

```
hnbgw-ranap schema hnbapuestats format "Number of paging requests sent on
RANAP from CS Core Network Connections: %cs-paging-req-tx%\nNumber of
paging requests sent on RANAP from PS Core Network Connections: %ps-
paging-req-tx%"
```

hnbgw-rtp schema

Configures bulk statistics schema for Real-Time Protocol (RTP) message statistics collection in HNB-GW session instance.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

hnbgw-rtp schema *schema_name* **format** *format_string*

no hnbgw-rtp schema *schema_name*

no

Removes the configured RTP schema.

schema_name

Specifies a name for the RTP schema to be used as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies a name for RTP schema format, to be used, followed by schema variables. *format_string* must be an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

This command defines schemas used for RTP messaging statistics collection. Multiple RTP schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the **hnbgw-rtp schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *rtp1stats1* that records the number of RTP uplink packets dropped and number of RTCP application report messages received on RTP link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rtp schema rtp1stats1 format "%vpnname%-%vpnid%-%servname%-%rtp-
uplink-pkts-dropped%-%rtcp-app-report-rx%"
```

hnbgw-rua schema

Configures bulk statistics schema for RANAP User Adaptation (RUA) protocol message statistics collection in HNB-GW session instance.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

hnbgw-rua schema *schema_name* **format** *format_string*

no hnbgw-rua schema *schema_name*

no

Removes the configured RUA schema.

schema_name

Specifies a name for the RUA schema to be used as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies a name for RUA schema format, to be used, followed by schema variables. *format_string* must be an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

This command defines schemas used for RUA protocol messaging statistics collection. Multiple RUA schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the **hnbgw-rua schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *rua1stats1* that records the number of CS-Connect messages received and sent on RUA link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rua schema rua1stats1 format "%vpnname%-%vpnid%-%servname%-%cs-
connect-rx%-%cs-connect-tx%"
```

hnbgw-sctp schema

Configures bulk statistics schema for Stream Control Transmission Protocol (SCTP) message statistics collection in HNB-GW session instance.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

hnbgw-sctp schema *schema_name* **format** *format_string*

no hnbgw-sctp schema *schema_name*

no

Removes the configured SCTP schema.

schema_name

Specifies a name for the SCTP schema to be used as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies a name for SCTP schema format, to be used, followed by schema variables. *format_string* must be an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

This command defines schemas used for SCTP protocol messaging statistics collection. Multiple SCTP schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the **hnbgw-sctp schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *sctp1stats1* that records the number of bytes received from lower layer and number of bytes sent to lower layer over SCTP connection along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-sctp schema sctp1stats1 format "%vpnname%-%vpnid%-%servname%-
%total-bytes-sent-to-lower-layer%-%total-bytes-rcvd-from-lower-layer%%"
```

hsgw schema

Configures HRPD Serving Gateway (HSGW) bulk statistics schema.

Product

HSGW

Privilege

Security Administrator, Administrator

Syntax

hsgw schema *schema_name* **format** *format_string*

no hsgw schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the format of the collected HSGW statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages. The format value comprises an alphanumeric string of 1 through 3599 characters.The format string syntax is described by Schema Format String Syntax .

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for HSGW bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple HSGW schemas can be created to categorize HSGW bulk statistics. All of the schemas are processed at each collection interval. To create multiple HSGW schemas, re-issue the **hsgw schema** *schema_name* command using a different schema name each time.

imsa schema

Configures IP Multimedia System Authorization (IMSA) bulk statistics schema.

Product

GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

Privilege

Security Administrator, Administrator

Syntax

imsa schema *schema_name* **format** *format_string*

no imsa schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the format of the collected IMSA statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages. The format value comprises an alphanumeric string of 1 through 3599 characters.The format string syntax is described by Schema Format String Syntax .

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for IMSA bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple IMSA schemas can be created to categorize IMSA bulk statistics. All of the schemas are processed at each collection interval. To create multiple IMSA schemas, re-issue the **imsa schema** *schema_name* command using a different schema name each time.

ippool schema

Configures IP pool bulk statistics schema.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ippool schema *schema_name* **format** *format_string*

no ippool schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for IP pool bulk statistics collection. Multiple IP pool schemas can be created to further categorize IP pool bulk statistics. All of the schemas are processed at each collection interval. To create multiple IP pool schemas, re-issue the **ippool schema** *schema_name* command using a different schema name.

Example

To create an IP pool schema named *ippoolstats* that specifies a schema format of:

- Number of IP addresses on hold: *hold*
- Number of free IP addresses: *free*

Use the following command:

```
ippool schema ippoolstats format "Number of IP addresses on hold:
%hold%\nNumber of free IP addresses: %free%\n"
```

ipsg schema

Configures IP Services Gateway (IPSG) bulk statistics schema.

Product

IPSG

Privilege

Security Administrator, Administrator

Syntax

ipsg schema *schema_name* **format** *format_string*

no ipsg schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define the schemas used for IPSG bulk statistics collection. Multiple IPSG schemas can be created to categorize IPSG bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the **ipsg schema** *schema_name* command using a different schema name.

Example

To create an IPSG schema named *ipsgstats* that specifies a schema format of:

- Context name: *vpnname*
- Service name: *servname*
- Total responses sent: *total-rsp-sent*

Use the following command:

```
ipsg schema ippoolstats format "Context name: %vpnname%\nService name:
%servname%\nTotal responses sent: %total-rsp-sent%\n"
```

lac schema

Configures LAC (L2TP Access Concentrator) bulk statistics schema.

Product

All

Privilege

Security Administrator, Administrator

Syntax

lac schema *schema_name* **format** *format_string*

no lac schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for LAC bulk statistics collection. Multiple LAC schemas can be created to categorize LAC bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the **lac schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *lac1stats1* that records the number of active subscriber sessions and the number of sessions that failed or were disconnected due to the maximum tunnel limit being reached:

```
lac schema lac1stats1 format "%sess-curactive%-%sess-maxtunnel%"
```

To create a schema called *lacresourcestats* that specifies a schema format of:

- Number of Successful Session Connections: *sess-successful*
- Number of Session Attempts That Failed: *sess-failed*
- Number of Sessions Currently Active: *sess-curative*

Use the following command:

```
lac schema lacresourcestats format "Number of Successful Session
Connections: %sess-successful%\nNumber of Session Attempts That Failed:
%sess-failed%\nNumber of Sessions Currently Active: %sess-curative%"
```

limit

Configures the maximum amount of system memory bulk statistics may utilize.

Product

All

Privilege

Security Administrator, Administrator

Syntax

limit *kilobytes*

kilobytes

Specifies the maximum amount of memory (in kilobytes) that may be used for bulk statistics as an integer from 1 through 32000. Default: 100

Usage

Adjust bulk statics memory usage when considering the sampling interval adjustments.

Caution: Bulk statistics are stored in Random Access Memory (RAM) on the SMC. In the event of power loss or system failure, the statistics will be lost. If the maximum storage limit has been reached before the system's configured transfer-interval is reached, the oldest information stored in the collection will be overwritten.

Example

```
limit 2048
```

lma schema

Configures the Local Mobility Anchor (LMA) statistics schema for the naming conventions of data files.

Product

P-GW

Privilege

Administrator

Syntax

lma schema *schema_name* **format** *format_string*

no lma schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name. as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for LMA bulk statistics collection. Multiple LMA service schemas can be created to categorize LMA service bulk statistics. All of the schemas are processed at each collection interval. To create multiple LMA service schemas, re-issue the **lma schema** *schema_name* command using a different schema name.

Example

For an LMA-level schema called *lmaservicestats* that specifies a schema format of:

- Binding Update Received: *bindupd*
- Binding Update Received - Denied: *bindupd-denied*

Use the following command:

```
lma schema lmaservicestats format "Number of Binding Updates Received:
%bindupd%\nNumber of Binding Updates Received and Denied: %bindupd-
denied%\n"
```

lns schema

Configures LNS (L2TP Network Server) bulk statistics schema.

Product

LNS

Privilege

Security Administrator, Administrator

Syntax

lns schema *schema_name* **format** *format_string*

no lns schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the format of the collected LNS statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages. The format value comprises an alphanumeric string of 1 through 3599 characters.The format string syntax is described by Schema Format String Syntax .

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for LNS bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple LNS schemas can be created to categorize LNS bulk statistics. All of the schemas are processed at each collection interval. To create multiple LNS schemas, re-issue the **lns schema** *schema_name* command using a different schema name each time.

local-directory

Sets the local directory for storing bulkstats collection files

Product

All

Privilege

Security Administrator, Administrator

Syntax

local-directory *pathname*

no local-directory

no

Delete the setting for local-directory.

pathname

Specifies the local path of the directory in which to store bulkstats collection files. This must be an alphanumeric string of 1 through 127 characters. Pathnames are case sensitive.

Usage

Use this command to designate a directory on a local file system in which collection files with bulkstats information are stored. The directory specified must already exist. Use the Exec Mode command **mkdir** to create a directory.

Example

To specify that bulkstats collection files are stored in the local directory */flash/bulkstats*, enter the following command:

```
local-directory /flash/bulkstats
```

mag schema

Configures the Mobile Access Gateway (MAG) statistics schema for naming conventions of data files.

Product

HSGW, S-GW

Privilege

Administrator

Syntax

mag schema *schema_name* **format** *format_string*

no mag schema *schema_name*

no

Removes the specified schema from MAG bulk statistics generation.

schema_name

Specifies the name to use to refer to the schema and associated format string. *schema_name* must be an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for MAG bulk statistics collection. Multiple MAG service schemas can be created to categorize MAG service bulk statistics. All of the schemas are processed at each collection interval. To create multiple MAG service schemas, re-issue the **mag schema** *schema_name* command using a different schema name.

Example

For a MAG-level schema called *magservicestats* that specifies a schema format of:

- Binding Update Sent: *bindupd*
- Binding Acknowledgement Received: *bindack*

Use the following command:

```
mag schema magservicestats format "Number of Binding Updates Sent:
%bindupd%\nNumber of Binding Acknowledgements Received: %bindack%\n"
```

mipv6ha schema

Configures MIPv6 HA (home Agent) bulk statistics schema.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

mipv6ha schema *schema_name* **format** *format_string*

no mipv6ha schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for MIPv6 HA bulk statistics collection. Multiple MIPv6 HA bulk statistics schemas can be created to categorize MIPv6 HA bulk statistics. All of the schemas are processed at each collection interval. To create multiple MIPv6 HA service schemas, re-issue the **mipv6ha schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *mipv6haservicestats* that records the number of authorization attempt failures due to access rejects from AAA:

```
mipv6ha schema mipv6haservicestats format "%aaa-actauthfail%"
```

mme schema

Configures MME (Mobility Management Entity) bulk statistics schema.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

mme schema *schema_name* **format** *format_string*

no mme schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for MME bulk statistics collection. Multiple MME bulk statistics schemas can be created to categorize MME bulk statistics. All of the schemas are processed at each collection interval. To create multiple MME service schemas, re-issue the **mme schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *mmeservice_s1ap_cfg_transfers* that records the total number of S1AP - transmit data - configuration transfers:

```
mme schema mmeservice_s1ap_cfg_transfersformat "s1ap-trnsdata-cfg-tfr
```

mvs schema

Configures MVS (Mobile Videoscape) bulk statistics schema.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

mvs schema *schema_name* **format** *format_string*

no mvs schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name. as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference.*

nat-realm schema

Creates and configures Network Address Translation (NAT) realm statistics schema.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

nat-realm schema *schema_name* **format** *format_string*

no nat-realm schema *schema_name*

schema_name

Specifies the NAT realm bulk statistics schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for NAT Realm bulk statistics collection. Multiple NAT realm schemas can be created to further categorize NAT realm level bulk statistics. All of the schemas are processed at each collection interval. To create multiple NAT Realm schemas, re-issue the **nat-realm schema** *schema_name* command using a different schema name.

Example

The following command creates a NAT realm schema with the VPN name, realm name, and flows information:

```
nat-realm schema realm1 format "%vpnname% %realmname% %nat-rlm-flows%"
```

pcc-af schema

Configures Policy and Charging Control-Application Function (PCC-AF) service bulk statistics schema.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

pcc-af schema *schema_name* **format** *format_string*

no pcc-af schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for PCC-AF service bulk statistics collection. Multiple PCC-AF service schemas can be created to categorize PCC-AF service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PCC-AF service schemas, re-issue the **pcc-af schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *pcc_af1stats1* that records the total number of Rx STR messages received and total number of Rx AAR Accept messages sent along with Context name, Context Id, and PCC-AF service name:

```
pcc-af schema pcc_af1stats1 format "%vpnname%-%vpnid%-%servname%-%total-
rx-ccai-accept-sent%-%total-rx-aar-accept-sent%"
```

pcc-policy schema

Configures Policy and Charging Control-Policy (PCC-Policy) service bulk statistics schema.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

pcc-policy schema *schema_name* **format** *format_string*

no pcc-policy schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for PCC-Policy service bulk statistics collection. Multiple PCC-Policy service schemas can be created to categorize PCC-Policy service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PCC-Policy service schemas, re-issue the **pcc-policy schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *pcc_plcy1stats1* that records the total number of Gx messages sent and total number of Gx CCR messages received along with Context name, Context Id, and PCC-Policy service name:

```
pcc-policy schema pcc_plcy1stats1 format "%vpnname%-%vpnid%-%servname%-
%total-gx-outbound-msgs%-%total-gx-ccr-rcvd%"
```

pcc-sp-endpt schema

Configures the bulkstats schema at the Sp interface endpoint for PCC procedures with Subscriber Service Controller/Subscriber Policy Register (SSC/SPR).

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

pcc-sp-endpt schema *schema_name* **format** *format_string*

no pcc-sp-endpt schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for PCC-Sp-Endpoint bulk statistics collection. Multiple PCC-Sp-Endpoint schemas can be created to categorize PCC-Sp-Endpoint bulk statistics. All of the schemas are processed at each collection interval. To create multiple PCC-Sp-Endpoint schemas, re-issue the **pcc-sp-endpt schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *pcc_sp1stats1* that records the total number of SPRMgr Sh session close and open requests received from PCCMgr and processed by PCC-Sp-Endpoint along with Context name, Context Id, and PCC-Sp-Endpoint name:

```
pcc-sp-endpt schema pcc_svc1stats1 format "%vpnname%-%vpnid%-%endpt-
name%-%req-open%-%req-close%"
```

pcc-service schema

Configures Policy and Charging Control-Service (PCC-Service) bulk statistics schema.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

pcc-service schema *schema_name* **format** *format_string*

no pcc-service schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for PCC-Service bulk statistics collection. Multiple PCC-Service schemas can be created to categorize PCC-Service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PCC-Service schemas, re-issue the **pcc-service schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *pcc_svc1stats1* that records the total number of Gx and Gy request processed by PCC-Service along with Context name, Context Id, and PCC-Service name:

```
pcc-service schema pcc_svc1stats1 format "%vpnname%-%vpnid%-%servname%-
%total-gx-processed%-%total-gy-processed%"
```

pdif schema

Configures Packet Data Interworking Function (PDIF) bulk statistics schema.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

pdif schema *schema_name* **format** *format_string*

no pdif schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3600 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for PDIF bulk statistics collection. Multiple PDIF schemas can be created to categorize PDIF bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the **pdif schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *pdifschema1* for the category current active ipv4 sessions:

```
pdif schema pdifschema1 format %sess-curactip4%
```

pgw schema

Configures Packet Data Network Gateway (P-GW) bulk statistics schema.

Product

P-GW

Privilege

Security Administrator, Administrator

Syntax

pgw schema *schema_name* **format** *format_string*

no pgw schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the format of the collected P-GW statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages. The format value comprises an alphanumeric string of 1 through 3599 characters.The format string syntax is described by Schema Format String Syntax .

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for P-GW bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple P-GW schemas can be created to categorize P-GW bulk statistics. All of the schemas are processed at each collection interval. To create multiple P-GW schemas, re-issue the **pgw schema** *schema_name* command using a different schema name each time.

port schema

Configures port bulk statistics schema.

Product

All

Privilege

Security Administrator, Administrator

Syntax

port schema *schema_name* **format** *format_string*

no port schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format. as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for port bulk statistics collection. Multiple port schemas can be created to categorize port-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple port schemas, re-issue the **port schema** *schema_name* command using a different schema name.

Important: The *card* variable in the Port schema is not supported on all platforms

Example

To create a port-level schema named *portstats1* that separates the *card/port*, *bcast_inpackets*, and *bcast-outpackets* variables by hyphens ("-"), enter the following command:

```
port schema portstats1 format "%card%/%port% - %bcast_inpackets% -
%bcast_outpackets%"
```

ppp schema

Configures Point-to-Point Protocol (PPP) bulk statistics schema.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ppp schema *schema_name* **format** *format_string*

no ppp schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for point-to-point protocol bulk statistics collection. Multiple PPP-service schemas can be created to categorize PPP-service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PPP-service schemas, re-issue the **ppp schema** *schema_name* command using a different schema name.

Example

To create a ppp-level schema named *pppstats* that specifies a schema format of:

- CHAP: (Challenge Handshake Authentication Protocol)
- Auth. Attempts: *auth-attempt-chapAuth*. Successes: *auth-success-chap*
- PAP: (Password Authentication Protocol)
- Auth. Attempts: *auth-attempt-papAuth*. Successes: *auth-success-pap*

Use the following command:

```
ppp schema pppstats format "CHAP:\nAuth. Attempts: %auth-attempt-
chap%\tAuth. Successes: %auth-success-chap%\nPAP:\nAuth. Attempts: %auth-
attempt-pap%\tAuth. Successes: %auth-success-pap%\n"
```

ps-network-ranap

Configures the Radio Access Network Application Part (RANAP) bulk statistics schema in Packet Switched (PS) network associated with an HNB-GW node.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

ps-network-ranap schema *schema_name* **format** *format_string*

no ps-network-ranap schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format. as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for RANAP procedure related bulk statistics collection in a PS network associated with HNB-GW in a Femto UMTS network. Multiple PS Networks RANAP schemas can be created to further categorize at PS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple PS Networks RANAP schemas, re-issue the **ps-network-ranap schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *ps_ranap1stats1* that records the total number of Iu Release Request messages transmitted and total number of Iu Release Command message received by HNB-GW node:

```
ps-network-ranap schema ps_ranaplstats1 format "%iu-rel-req-tx%" "%iu-rel-cmd-rx%"
```

radius schema

Configures RADIUS bulk statistics schema.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

radius schema *schema_name* **format** *format_string*

no radius schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters that is case sensitive.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for RADIUS bulk statistics collection. Multiple RADIUS schemas can be created to categorize RADIUS bulk statistics. All of the schemas are processed at each collection interval. To create multiple RADIUS schemas, re-issue the **radius schema** *schema_name* command using a different schema name.

Example

To create a RADIUS schema named *radius_statistics* that specifies a schema format of:

- Server: *ipaddr*
- Authentication Requests Sent: *auth-req-sent*
- Accounting Requests Sent: *acc-req-sent*

Use the following command:

```
radius schema radius_statistics format "Server: %ipaddr%\nAuthentication
Requests Sent: %auth-req-sent%\nAccounting Requests Sent: %acc-req-sent%"
```

receiver

Configures a host system to receive bulkstats information through Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP) or SSH File Transfer Protocol (SFTP).

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
receiver { mode { redundant | secondary-on-failure } | ip_address { primary | secondary }
[ mechanism { { { ftp | sftp } login user_name [ encrypted ] password pwd } | tftp } } ]
}

no receiver ip_address
```

no

Removes the receiver specified from the list of receivers where data files are sent.

mode { redundant | secondary-on-failure }

Determines how bulkstats are delivered to the primary and secondary receivers.
Default: **secondary-on-failure**
redundant: Files are transferred to both the primary and secondary receivers. If either transfer is not currently possible, the file is transferred when possible. The system continues to hold in memory as much data as possible until the data has been successfully transferred to both receivers. Data is only discarded if the in-memory data reaches the configured limit. Refer to the **limit** command.
secondary-on-failure: Files are transferred to the secondary receiver if the primary receiver fails. In-memory data is erased once the data is transferred to either the primary or secondary receiver. This is the default behavior.

ip_address

Specifies the IP address of the receiver of interest using IPv4 dotted-decimal notation.

primary | secondary

Primary and secondary are used to indicate the order in which receivers are connected. The secondary is used when the primary is unreachable.
primary: indicates the receiver is the primary receiver of data.
secondary: indicates the receiver is the secondary receiver of data.

mechanism { { { ftp | sftp } login *user_name* **[encrypted] password** *pwd* **} | tftp } }**

Specifies the method by which data is transferred to the receiver.
ftp login *user_name* [**encrypted**] **password** *pwd*: the FTP protocol shall be used for data file transfer. *user_name* specifies the user to provide for remote system secure logins and must be an alphanumeric string of 1 through 31 characters. The password to use for remote system authentication is specified as *pwd* and must be from 1 to 31 characters or 1 to 64 characters if the **encrypted** keyword is also specified.

sftp login *user_name* [**encrypted**] **password** *pwd*: the SFTP protocol shall be used for data file transfer. *user_name* specifies the user to provide for remote system secure logins and must be an alphanumeric string of 1 through 31 characters. The password to use for remote system authentication is specified as *pwd* and must be from 1 to 31 characters or 1 to 64 characters if the **encrypted** keyword is also specified.
tftp: the TFTP protocol is to be used to transfer files.
The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

Usage

Use TFTP methods to reduce transfer times if excessive system resources are being used across the network for transfer of data.
FTP transfer method allows for login which then provides system logging within the enabled FTP logs.
The initial connection is attempted to the primary receiver. If the primary receiver is unreachable for any reason, the secondary receiver is used. If the secondary receiver is also unreachable, the system retries after a delay period where it again attempts to connect to the primary receiver followed by the secondary receiver as necessary.

Important: For redundant receivers, configuration changes to the receivers are applied to all existing and all subsequent data sets pending transfer. If no receiver is configured, bulk statistics will be collected and stored on the system until the maximum amount of memory is used; they will not be transferred to the receiver(s). When the storage limit has been reached the oldest information is overwritten. When a receiver is configured for the primary and secondary target, this command will use both receivers as default if no receiver is specified.

Example

```
receiver 10.2.3.4 primary mechanism tftp

receiver 10.2.3.5 secondary

no receiver 10.2.3.4
```

remotefile

Configures the naming convention with support for multiple file format to multiple receivers when storing the data files on the remote receiver(s).

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
remotefile format format_string [ both-receivers | primary-receiver | secondary-receiver
]

no remotefile format
```

no

Resets the remote file naming convention to the system default.

format *format_string*

Specifies the naming convention format to use as an alphanumeric string of 1 through 127 characters. The format string syntax is described in the Schema Format String Syntax section. Default: "%date%-%time%"

Important: The remote file naming format should only use static text and bulk statistic variables to avoid any possible file creation issues on the receivers.

The following variables are supported:

Table 13. remote file Command Naming Format Variables

Variable	Description	Data Type
date	The UTC date that the collection file was created in YYYYMMDD format where YYYY represents the year, MM represents the month and DD represents the day.	String
date3	The UTC date that the collection file was created in YYMMDD format where YY represents the year, MM represents the month and DD represents the day.	String
host	The system hostname that created the file	String
sysuptime	The uptime (in seconds) of the system that created the file.	32-bit signed
time	The time that the collection file was created in HHMMSS format where HH represents the hours, MM represents the minutes, and SS represents the seconds.	String

both-receivers | primary-receiver | secondary-receiver

Sets the remote file creation target to both receivers, primary receiver or secondary receiver. Default: Both receivers.

Usage

Set the remote file naming format to ensure consistent data file naming across a network or adjusting a single system's format for easy identification.
This command specifies whether the format should be used in conjunction with both receivers, only the primary receiver, or only the secondary receiver.

Important: For redundant receivers, the filenames for the output data files are applied when the information is first gathered. If the name format is modified, the change takes effect for the next data set. The current data set name remains unchanged. even if has not yet been transferred.

Example

```
remotefile format simpleFormat

remotefile format "%host%-%date%-%time%"

remotefile format "%host%-%date%-%time%" both-receivers

remotefile format "%host%-%date%" primary-receiver

no remotefile format
```

rp schema

Configures R-P bulk statistics schema.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

rp schema *schema_name* **format** *format_string*

no rp schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for R-P bulk statistics collection. Multiple PDSN service schemas can be created to categorize PDSN service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PDSN service schemas, re-issue the **rp schema** *schema_name* command using a different schema name.

Example

To create an PDSN-level schema called *pdsnservicestats* that specifies a schema format of:

- Date: *date*
- Time: *time*
- Number of Authentication Denials: *deny-auth*

Use the following command:

```
rp schema rpservicestats format "Date: %date%\nTime: %time%\nNumber of
Authentication Denials: %deny-auth%\n"
```

sample-interval

Configures the time interval between collecting local statistics.

Product

All

Privilege

Security Administrator, Administrator

Syntax

sample-interval *minutes*

minutes

Specifies the frequency (in minutes) of polling for local statistics as an integer from 1 through 1440.

Usage

Adjust the sampling interval to tune the system response as shorter periods can cause undue system overhead whereas longer periods have less of a statistical importance when analyzing data.
The system is shipped from the factory with the sampling interval set to 15 minutes.

Example

```
sample-interval 120
```

sccp schema

Configures the collection of statistics for the SCCP schema.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

sccp schema *sccp_schema_name* **format** *sccp_schema_format*

no sccp schema *sccp_schema_name*

no

Removes the specified schema.

sccp_schema_name

Specifies a name for a model collection schema for SCCP statistics. The name must be comprised of an alphanumeric string of 1 to 31 characters.

format *sccp_schema_format*

Specifies the format of the collected SCCP statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages. The format value comprises an alphanumeric string of 1 through 3599 characters. For syntax details, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for the SCCP schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for SCCP bulk statistics collection in the generated stats report files.. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple SCCP schemas can be created to categorize SCCP bulk statistics. All of the schemas are processed at each collection interval. To create multiple SCCP schemas, re-issue the **sccp schema** *sccp_schema_name* command using a different schema name each time.

Example

Include the bulk statistic variable names to create an SCCP schema named *sccpstats11* that specifies collection of statistics (a schema format) for:

- Subsystem available messages sent from the SCCP
- Subsystem available messages received by the SCCP

Use the following command:

```
sccp schema sccpstats11 format "Subsys avail SCCP Tx: %ssa-txed%\nSubsys
avail SCCP Rx: %ssa-rcvd%\n"
```

schema

Configures the system-level bulk statistics schema.

Product

All

Privilege

Security Administrator, Administrator

Syntax

schema *schema_name* **format** *format_string*

no schema *schema_name*

no

Removes the specified schema.

schema_name

Specifies the schema name as an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the schema format as an alphanumeric string of 1 through 3599 characters. For syntax details, see Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for system-level bulk statistics collection. Multiple schemas can be created to categorize system-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple system schemas, re-issue the **schema** *schema_name* command using a different schema name.

Example

The following command creates a schema called *systemstats1* that records the number of current Simple IP and the number of current Mobile IP sessions:

```
schema systemstats1 format "%sess-cursipconn% - %sess-curmipconn%"
```

To create a system-level schema called *bulksysstats* that specifies a schema format of:

- Number of currently active sessions: *sess-curactcall*
- Number of currently dormant sessions: *sess-curdormcall*

Use the following command:

```
schema bulksysstats format "Number of currently active sessions: %sess-
curactcall%\nNumber of currently dormant sessions: %sess-curdormcall%\n"
```

sgs schema

Configures the collection of statistics for the SGs schema.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

sgs schema *schema_name* **format** *format_string*

no sgs schema *schema_name*

no

Removes the specified SGs schema from statistics collection.

schema_name

Specifies the name to use to refer to the schema and associated format string. *schema_name* must be an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the format of the collected SGs statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages. The format value comprises an alphanumeric string of 1 through 3599 characters. The format string syntax is described by Schema Format String Syntax .

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for SGs bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple SGSN schemas can be created to categorize SGSN bulk statistics. All of the schemas are processed at each collection interval. To create multiple SGSN schemas, re-issue the **sgs schema** *sgs_schema_name* command using a different schema name each time.

Example

Include the bulk statistic variable names to create an SGs schema named *stats_SGs_release* that specifies a collection of statistics (a schema format) for the total number of release messages transmitted, retransmitted, and received:
Use the following command:

```
sgs schema stats_SGs_release format "Total transmitted: %rel-req-
tx%\nTotal retransmitted: %rel-req-retx%\nTotal received: %rel-req-rx%\n"
```

sgsn schema

Configures the collection of statistics for the SGSN schema.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sgsn schema *schema_name* **format** *format_string*

no sgsn schema *schema_name*

no

Removes the specified SGSN schema from statistics collection.

schema_name

Specifies the name to use to refer to the schema and associated format string. *schema_name* must be an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the format of the collected SGSN statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages. The format value comprises an alphanumeric string of 1 through 3599 characters. The format string syntax is described by Schema Format String Syntax .

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for SGSN bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple SGSN schemas can be created to categorize SGSN bulk statistics. All of the schemas are processed at each collection interval. To create multiple SGSN schemas, re-issue the **sgsn schema** *sgsn_schema_name* command using a different schema name each time.

Example

Include the bulk statistic variable names to create an SGSN schema named *stats_3Gsgsn1* that specifies collection of statistics (a schema format) for the total number of 3G Attaches per LAC/RAC per MCC& MNC:
Use the following command:

```
sgsn schema stats_3Gsgsn1 format "MCC: %mcc%\nMNC: %mnc%\nLAC:
%lac%\nRAC: %rac%\nTotal 3G Subs Attached: %3G-attached%\n"
```

sgtp schema

Configures the collection of the SGSN's GTP-C and GTP-U activity statistics.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sgtp schema *schema_name* **format** *format_string*

no sgtp schema *schema_name*

no

Removes the specified SGTP schema from statistics collection.

schema_name

Specifies a name for a model collection schema for SGTP statistics. *schema_name* must be an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the format of the collected SGTP statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages. The format value comprises an alphanumeric string of 1 through 3599 characters.The format string syntax is described by Schema Format String Syntax .

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for SGTP bulk statistics collection in the generated stats report files.. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple SGTP schemas can be created to categorize SGTP bulk statistics. All of the schemas are processed at each collection interval. To create multiple SGTP schemas, re-issue the **sgtp schema** *sgtp_schema_name* command using a different schema name each time.

Example

Include the bulk statistic variable names to create an SGTP schema named *sgtpstats_sgsn1* that specifies collection of statistics (a schema format) will be by IuPS service interface and by RNC for the total number of GTP-C Create PDP Context Request messages received.
Use the following command:

```
sgtp schema sgtpstats_sgsn1 format "IuPS Service ID: %iups-service%\nRNC:
%rnc-address%\nTotal CPCR Rx: %sgtpc-total-cpc-req%\n"
```

sgw schema

Configures the collection of the S-GW activity statistics.

Product

S-GW

Privilege

Administrator

Syntax

sgw schema *schema_name* **format** *format_string*

no sgw schema *schema_name*

no

Removes the specified S-GW schema from statistics collection.

schema_name

Specifies a name for a model collection schema for S-GW statistics. *schema_name* must be an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the format of the collected S-GW statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages. The format value comprises an alphanumeric string of 1 through 3599 characters.The format string syntax is described by Schema Format String Syntax .

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for S-GW bulk statistics collection in the generated stats report files.. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple S-GW schemas can be created to categorize S-GW bulk statistics. All of the schemas are processed at each collection interval. To create multiple S-GW schemas, re-issue the **sgw schema** *sgw_schema_name* command using a different schema name each time.

Example

Include the bulk statistic variable names to create an S-GW schema named *sgwstats_sgw1* that specifies collection of statistics (a schema format) will be by S-GW service interface for the total number of currently idle and active UEs.
Use the following command:

```
sgw schema sgwstats_sgw1 format "SGW Service ID: %servname%\nTotal
Current Idle Ues: %sessstat-totcur-ueidle%\nTotal Current Active Ues:
%sessstat-totcur-ueactive%\n"
```

show variables

Displays the bulk statistics variable information based on schema names.

Product

All

Privilege

Security Administrator, Administrator

Syntax

show variables [*schema_name* **] [obsolete]**

---

show variables *schema_name*

Displays all valid bulkstat schema statistics, or only the statistics for the specified schema. *schema_name* specifies the name of the schemas available on the system. Following is the list of available schemas in this release.

- aal2
- alcap
- apn
- asngw
- asnpc
- bcmcs
- card
- closedrp
- common
- context
- cs-network-ranap
- cs-network-rtp
- cscf
- cscfintf
- dcca
- diameter-acct
- diameter-auth
- dlci-util
- dpca
- ecs
- egtpc
- epdg

- fa
- fng
- gprs
- gtpc
- gtpp
- gtpu
- ha
- hnbgw-hnbap
- hnbgw-ranap
- hnbgw-rtp
- hnbgw-rua
- hnbgw-sctp
- hsgw
- imsa
- ippool
- ipsg
- lac
- lma
- lns
- mag
- map
- mipv6ha
- mme
- mvs
- nat-realm
- pcc-af
- pcc-policy
- pcc-service
- pcc-sp-endpt
- pdg
- pdif
- pgw
- phsgw
- phspc

- port
- ppp
- ps-network-ranap
- radius
- rp
- sccp
- sgs
- sgsn
- sgtp
- sgw
- ss7link
- ss7rd
- system
- vpn

obsolete

Displays obsolete (but still available) schema variables. An asterisk (*) is displayed next to schema variables that have been obsoleted.

Usage

Use this command to list supported bulk statistic variables. Variables can be listed for a specified schema. If no schema is specified, all supported variables are listed on a per-schema basis.

Example

The following command displays the bulkstat variables only for the card schema:

```
show variables card
```

ss7link schema

Configures the collection of the SS7 link activity statistics.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ss7link schema *schema_name* **format** *format_string*

no ss7link schema *schema_name*

no

Removes the specified SS7 Link schema from statistics collection.

schema_name

Specifies the name to use to refer to the schema and associated format string. *schema_name* must be an alphanumeric string of 1 through 31 characters.

format *format_string*

Specifies the naming convention format to use. *format_string* must be an alphanumeric string of 1 through 3599 characters. The format string syntax is described by Schema Format String Syntax .

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for SS7 link and linkset bulk statistics collection per SS7 routing domain in a generated stats report file. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple collection schemas can be created to categorize SS7 link bulk statistics. All of the schemas are processed at each collection interval. To create multiple SS7 link schemas, re-issue the **ss7link schema** *ss7link_schema_name* command using a different schema name each time.

Example

The following command creates a schema called *ss7lnk1stats1* that records the changeover orders sent and received per linkset and link and per SS7 routing domain:

```
ss7link schema ss7lnk1stats1 format "%ss7rd-number%-%ss7-linkset-id%-
%ss7-link-id%-%ss7rd-asp_instance%-%ss7-link-mtp3-changeover-order-tx%-
%ss7-link-mtp3-changeover-order-rx%"
```

ss7rd schema

Configures the collection of bulk statistics for SS7 routing domain services, which include the activity statistics for SCTP, MTP, and M3UA data.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

ss7rd schema *schema_name* **format** *format_string*

no ss7rd schema *schema_name*

no

Removes the specified SS7 routing domain schema from statistics collection.

schema_name

Specifies the name to use to refer to the model collection schema and the associated format string. *schema_name* must be an alphanumeric string of 1 to 31 characters.

format *format_string*

Specifies the format of the collected SS7 routing domain statistics by identifying the statistics variables and the ordering of the variables for presentation within the bulk statistics collection report. The format value comprises an alphanumeric string of 1 through 3599 characters.The format string syntax is described by Schema Format String Syntax .

Important: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

Usage

Use this command to define schemas for collection of SS7 routing domain statistics to be included in the generated stats report file. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple collection schemas can be created to categorize SS7 routing domain bulk statistics. All of the schemas are processed at each collection interval. To create multiple SS7 routing domain schemas, re-issue the **ss7rd schema** *ss7rd_schema_name* command using a different schema name each time.

Example

The following command creates a schema called *ss7rd1stats1* that identifies the SS7 routing domain and records the Application Server Process instance in the SS7 routing domain, along with the total number of sent and received SHUTDOWN messages per SS7 routing domain:

```
ss7rd schema ss7rd1stats1 format "%ss7rd-number%-%ss7rd-asp_instance%-
%ss7rd-sctp-shutdown-tx%-%ss7rd-sctp-shutdown-rx%"
```

transfer-interval

Configures the frequency of transfer of collected statistics to the receiver.

Product

All

Privilege

Security Administrator, Administrator

Syntax

transfer-interval *minutes*

minutes

Specifies the number of minutes between the transfer of collected statistics to the receivers as an integer from 1 through 999999.

Usage

Modify the transfer interval based upon the number of sessions per second. As the number of session requests a second increases it may become necessary to increase the transfer interval to reduce the processing overhead frequency for statistics delivery. This is tempered by the impact reduced resolution of statical data has on usefulness of data when the interval gets larger than the least busy hours and most busy hours of the day.

The system is shipped from the factory with the transfer interval set to 480 minutes.

Example

```
transfer-interval 1440
```

Chapter 43
Call Control Profile Configuration Mode

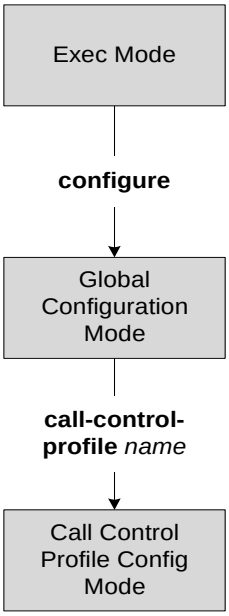
Call Control Profile configuration mode defines call-handling rules which can be combined with other profiles – such as an APN profile (see the *APN Profile Configuration Mode Commands* chapter) – when using the Operator Policy feature. The call control profile is a key element in the Operator Policy feature and the profile is not valid until it is associated with an operator policy (see the *Operator Policy Configuration Mode Commands* chapter).

The MME and SGSN each support a maximum of 1,000 call control profiles; only one profile can be associated with an operator policy.

By configuring a call control profile, the operator fine tunes any desired restrictions or limitations needed to control call handling per subscriber or for a group of callers across IMSI (International Mobile Subscriber Identity) ranges.

Upon accessing this mode, the CLI prompt be similar to the following:

```
[local]asr5000(config-call-control-profile-<profile_name>)#
```



access-restriction-data

Enables the operator to assign a failure code to be included in reject messages if the attach rejection is due to access restriction data (ARD) checking in the incoming subscriber data (ISD) messages. The operator can also disable the ARD checking behavior.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

access-restriction-data { failure-code *cause_code* **| no-check }**

remove access-restriction-data failure-code

---

remove

Removes the failure code setting for the reject message that could result from ARD checking.

---

failure-code *cause_code*

cause_code: Enter an integer from 2 through 111; default code is 13 (roaming not allowed in this location area [LA]).
Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable

- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

no-check

Including this keyword with the command disables the ARD checking behavior.

Usage

By default, the SGSN checks access restriction data (ARD) within incoming insert subscriber data (ISD) messages. This enables operator to selectively restrict subscribers in either 3G (UTRAN) or 2G (GERAN). The SGSN ARD checking behavior occurs during the attach procedure and if a reject occurs, the SGSN sends the subscriber an Attach Reject message with a configurable failure cause code.

Example

For this call control profile, the following command disables the ARD checking function:

```
access-restriction-data no-check
```

accounting context

Defines the name of the accounting context and optionally associates a GTPP group with this call control profile.

Product

SGSN, S-GW

Privilege

Security Administrator, Administrator

Syntax

accounting context *ctxt_name* **[gtpp group** *grp_name* **]**

remove accounting context

remove

Removes the accounting configuration from this profile's configuration.

ctxt_name

Specifies the accounting context as an alphanumeric string of 1 through 79 characters.

gtpp group *grp_name*

Identifies the GTPP group, where the GTPP related parameters have been configured in the GTPP Group Configuration mode, to associate with this call control profile.
grp_name: Enter an alphanumeric string of 1 through 63 characters to identify the GTPP group created with the **gtpp group** command in the Context configuration mode.

Usage

This command can be used to associate a predefined GTPP server group - including all its associated configuration - with a specific call control profile. The GTPP group would have been defined with the **gtpp group** command (see the *Context Configuration Mode Commands* chapter).
If the GTPP group is not specified, then a default GTPP group in the accounting context will be used.
If this command is not specified, use the name of the accounting context configured in the SGSN service configuration mode (for 3G) or the GPRS service configuration mode (for 2G), either will automatically use a "default" GTPP group generated in that accounting context.
If the accounting context is specified in the GPRS service or SGSN service and in a call control profile, the priority is given to the accounting context of the call control profile.

Example

For this call control profile, the following command identifies an accounting context called *acctng1* and associates a GTPP server group named *roamers* with defined charging gateway accounting functionality.

```
accounting context acctng1 gtpp group roamers
```

accounting mode

Configures the mode to be used for accounting – GTPP (default), RADIUS/Diameter or None.

Product

S-GW

Privilege

Administrator

Syntax

```
[ default ] accounting mode { gtpp | none | radius-diameter }
```

default accounting mode

Sets the accounting mode to GTPP.

gtpp

Specifies that GTPP accounting is performed. This is the default method.

none

Specifies that no accounting will be performed for the call control profile.

radius-diameter

Specifies that RADIUS/Diameter will be performed for the call control profile.

Usage

Use this command to specify the accounting mode for a call control profile. For additional information on accounting mode and its relationship to operator policy, refer to the *System Administration Guide*.

Example

The following command specifies that RADIUS/Diameter accounting will be used for the call control profile:

```
accounting mode radius-diameter
```

allocate-ptmsi-signature

Enables or disables the allocation of a P-TMSI (Packet Temporary Mobile Subscriber Identity) signature.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] allocate-ptmsi-signature
```

no

Disables the allocation of the P-TMSI signature.

default

Resets the configuration value to the default: allocates the P-TMSI signature.

Usage

Use this command to enable or disable the allocation of the P-TMSI signature.

Example

```
allocate-ptmsi-signature
```

apn-restriction

Enables the APN restriction feature and configures the instruction for the SGSN on the action to take when an APN restriction value is received from the GGSN during an Update PDP Context procedure.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

apn-restriction update-policy deactivate *restriction*

default apn-restriction

default

Creates a default APN restriction configuration.

update-policy deactivate *restriction*

Specifies one of the two restriction types to define the appropriate action if the APN restriction value received conflicts with the stored value:

- **least-restrictive:** least restrictive value applicable when there are no already active PDP context(s).
- **most-restrictive:** most restrictive is the most stringent restriction required by any already active PDP context(s).

Usage

When this feature is enabled, the SGSN will send the maximum APN restriction value in every CPC Request message sent to the GGSN. The SGSN expects to receive an APN restriction value in each PDP Context received from the GGSN. The SGSN stores and compares received APN restriction values to check for conflicts. In the case of a conflict, the SGSN rejects the PDP Context with appropriate messages and error codes to the MS.
If an APN restriction value is not assigned by the GGSN, the SGSN assumes the value of "1" (least restrictive) to allow APN restriction rules will be possible when valid values are assigned for new PDP Context(s) from the same MS.

Example

The following command applies the lowest level of APN restrictions:

```
apn-restriction update-policy deactivate least-restrictive
```

associate

Associates various MME-specific lists and databases with this call control profile.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

associate { ho-restrict-list *list_name* **| hss-peer-service** *service_name* **[s13-interface | s6a-interface] | tai-mgmt-db** *tai-db_name* **}**

remove associate { ho-restrict-list | hss-peer-service [s13-interface | s6a-interface] | tai-mgmt-db }

remove

Remove the specified association definition from the call control profile.

ho-restrict-list *list_name*

Identifies the handover restriction list that should be associated with this call control profile. *list_name* is an alphanumeric string of 1 through 64 characters.

hss-peer-service *service_name*

Associates a Home Subscriber Server (HSS) peer service with this call control profile. *service_name* is an existing HSS peer service expressed as an alphanumeric string of 1 through 63 characters.

[s13-interface | s6a-interface]

Optionally, identify the interface to be associated with the HSS service in this call control profile.

tai-mgmt-db *tai-db_name*

Identifies the tracking area identifier (TAI) database that should be associated with this call control profile. *tai-db_name* is an alphanumeric string of 1 through 64 characters.
This configuration overrides the S-GW selection and TAI list assignment functionality for a call that uses an operator policy associated with this call control profile. The TAI management object provides a TAI list for calls and provides S-GW selection functionality if a DNS is not configured for S-GW discovery for this operator policy or if a DNS discovery fails.

Usage

Use this command to associate handover restriction lists, HSS service (and interfaces), and TAI dB with the call control profile. This ensures that the information is available for application when a Request is received. Repeat the command as needed to associate each feature.

Example

Link HO restriction list named *HOrestrict1* with this call control profile:

```
associate ho-restrict-list HOrestrict1
```

attach

Defines attach-related configuration parameters for this call control profile.

Important: SGSN only: Before using this command, ensure that the appropriate location area code (LAC) information has been defined via the **location-area-list** command.

Product

MME, SGSN

Privilege

Security Administrator, Administrator

Syntax

attach access-type { gprs | umts } { all | location-area-list instance *list_id* **} { failure-code** *code* **| user-device-release { before-r99 failure code** *code* **| r99-or-later failure code** *code* **} }**

default attach access-type { gprs | umts } { all | location-area-list instance *list_id* **} { failure-code | user-device-release { before-r99 failure code | r99-or-later failure code }**

[no] attach allow access-type { eps | gprs | umts } location-area-list instance *list_id*

[no] attach restrict access-type { eps | gprs | umts } { all | location-area-list instance *list_id* **}**

attach imei-query-type { imei | imei-sv | none } [[verify-equipment-identity] [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]

remove attach imei-query-type

default

Restores the default values for the for the specified parameter.

no

Deletes the specified attach configuration.

remove

Deletes the specified attach configuration.

access-type *type*

Defines the type of access to be allowed or restricted.

- **eps**
- **gprs**
- **umts**

If this keyword is not included, then both access types are allowed by default.

allow

Allow re-enables attaches in the configuration after an **attach restrict** command has been used.

restrict

Restrict attaches (do not accept calls) of specified **access-type** and from specified location areas (defined using either the **all** or **location-area-list** keywords).

all

Instructs the SGSN or MME to apply the command action to all location area lists. Location area lists should already have been created with the **location-area-list** command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.

location-area-list instance *list_id*

Instructs the MME or SGSN to apply the command action to a specific location area list. Location area lists should already have been created with the **location-area-list** command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.
Using this keyword with either the **allow** or **restrict** keywords enables you to configure with more granularity.
list_id: Enter an integer between 1 and 5.

failure-code *code*

Specify a GMM failure cause code to identify the reason an attach did not occur. This GMM cause code will be sent in the reject message to the MS.
Default: 14.
fail-code: Enter an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion

- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

---

user-device-release { before-r99 | r99-or-later } failure-code *code*

Default: disabled
Enables the SGSN to reject an Attach procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber's IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile are found that relate to this Attach Request.
3. Profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

- **r99-or-later** : Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

---

imei-query-type { imei | imei-sv | none }

This keyword set is specific to the MME.
Defines device Attach limitations if an IMEI is not already present in the Attach Request.

- **imei**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).

- **none**: Specifies that the MME does not need to query for IMEI or IMEI-SV.

verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]

Specifies that the identification (IMEI or IMEI-SV) of the UE is to be performed by the Equipment Identity Register (EIR) over the S13 interface.

- **allow-on-eca-timeout**: Configures the MME to allow equipment that has timed-out on ECA during the attach procedure.
- **deny-greylisted**: Configures the MME to deny grey-listed equipment during the attach procedure.
- **deny-unknown**: Configures the MME to deny unknown equipment during the attach procedure.
- **verify-emergency**: Configures the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases. This keyword is only supported in release 12.2 and higher.

Usage

Once the IMSI of an incoming call is known and matched with a specific operator policy, according to the filter definition of the **mcc** command, then the associated call control profile is selected to determine how the incoming call is handled.
By default, all attaches are allowed. If no access limitations are needed, then do not use the **attach** command.

Important: Before using this command, ensure that the appropriate LAC information has been defined with the **location-area-list** command.

Use this command to define attach limitations for the call control profile.
Use this command to fine-tune the attach configuration specifying which calls/subscribers can attach and which calls are restricted from attaching and what failure code is included in the Reject message.
Attachment restrictions can be based on any one or combination of the options, such as location area code or access type. It is even possible to restrict all attaches.
The command can be repeated using different keyword values to further fine-tune the attachment configuration.

Example

For calls under the purview of this call control profile, the following command restricts the attaches of **all** subscribers using the GPRS access type.

```
attach restrict access-type gprs all
```

Use the next command to reverse the previous attach restrict command:

```
attach allow access-type gprs all
```

Or, change the attach restriction to only restrict attaches of GPRS subscribers from specified LACs included in location area list #2 and include failure-code 45 as the reject cause. This configuration requires two CLI commands:

```
attach restrict access-type gprs location-area-list instance 2

attach access-type gprs location-area-list instance 2 failure-code 45
```

In the case of a dual-access SGSN, it is possible to also add a second definition to restrict attaches of UMTS subscribers within the LACs included in location area list #3.

```
attach restrict access-type UMTS location-area-list instance 3
```

Change the configuration to allow attaches for GPRS access for all previously restricted LACs - note that GPRS attaches would still be limited:

```
no attach restrict access-type gprs all
```

Restrict (deny) all GPRS attach requests (coming from any location area) and assign a single failure code for the reject messages. This is a two command process:

```
attach restrict access-type gprs all

attach access-type grps all failure-code 22
```

Remove the restrictions defined above - so that the access type is reset to the default (both types) and the failure code returns to the default value (14).

```
default attach access-type gprs all failure-code
```

authenticate activate

Allows the operator to define authentication procedures in response to a received Activate Request.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
authenticate activate [ access-type { gprs | umts } | first | frequency frequency |
primary ] [ access-type { gprs | umts } ]

[ no | remove ] authenticate activate [ access-type { gprs | umts } | first | primary ] [
access-type { gprs | umts } ] ]
```

no

Disables the specified activate authentication configuration in the call control profile.

remove

Removes the specified activate authentication configuration from the call control profile configuration file.

access-type *type*

One of the following must be selected to identify the type of network access if the **access-type** keyword is included in the command:

- **gprs**
- **umts**

The **access-type** keyword can be included with any of the other three keywords available with the **authenticate activate** command.

first

Including this keyword enables authentication only for the first Activate Request for an MS/UE.

frequency *frequency*

This keyword defines 1-in-N selective authentication for Activate Request events. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the twelfth event. *frequency* must be an integer from 1 to 16.

primary

Including this keyword enables authentication for every primary PDP context Activate Request.

Usage

Activate Requests are not authenticated by default. Use this command to enable authentication of Activate Requests.

Repeat the commands as needed to configure desired authentication responses to Activate Request messages for this call control profile.

Example

Configure Request Activate authentication for every primary PDP context for MS with GPRS access:

```
authenticate activate primary access-type gprs
```

authenticate all-events

Allows the operator to quickly define authentication procedures, based on limited parameters, for all types of events.

Product

MME, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
authenticate all-events [ access-type { gprs | umts } | frequency frequency [ access-type
{ gprs | umts } ] ]

[ no | remove ] authenticate all-events [ access-type { gprs | umts } ]
```

no

Disables the specified authentication configuration in the call control profile.

remove

Removes the specified authentication configuration from the call control profile configuration file.

access-type *type*

One of the following must be selected to identify the type of network access if the **access-type** keyword is included in the command:

- **gprs**
- **umts**

The **access-type** keyword can be included with any of the other three keywords available with the **authenticate all-events** command.

frequency *frequency*

This keyword defines 1-in-N selective authentication for all types of subscriber events. If the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the 12th event. *frequency* must be an integer from 1 to 16.

Usage

By default, authentication is not performed for any subscriber events. Use this command to enable authentication for all types of events at one time, such as but not limited to: Activate Requests, Attach Requests, Detach Requests, Service-Requests.

Example

The following command configures all authentication for all subscriber events to occur every tenth time a specific type of event occurs (for example every tenth time an Attach Request is received):

```
authenticate all-events frequency 10
```

The following command configures authentication for all Detach Requests and RAUs to occur if the UE access-type is UMTS:

```
authenticate all-events access-type umts
```

authenticate attach

Allows the operator to define authentication for Attach procedures.

Product

MME, SGSN

Privilege

Security Administrator, Administrator

Syntax

authenticate attach access-type { gprs | umts }

authenticate attach attach-type { combined | gprs-only } [access-type { gprs | umts } | frequency *frequency* **]**

authenticate attach frequency *frequency* **[access-type { gprs | umts }]**

authenticate attach inter-rat [access-type { gprs | umts } | attach-type { combined | gprs-only } [access-type { gprs | umts } | frequency *frequency* **] | frequency** *frequency* **[access-type { gprs | umts }]**

[no | remove] authenticate attach [access-type { gprs | umts } | attach-type { combined | gprs-only } | inter-rat | attach-type { combined | gprs-only }] [access-type { gprs | umts }]]

no

Disables the defined authentication procedures configured for Attach Requests from the call control profile.

remove

Deletes the defined authentication procedures for Attach Requests from the call control profile configuration file.

access-type *type*

One of the following must be selected to identify the type of network access if the **access-type** keyword is included in the command:

- **gprs**
- **umts**

attach-type

This keyword configures the Attach authentication based on the type of attach requested. The **attach-type** must be one of the following options:

- **combined**: Authenticates combined GPRS/IMSI Attaches.
- **gprs-only**: Authenticates GRPS Attaches only.

frequency *frequency*

This keyword defines 1-in-N selective authentication for this type of subscriber event - Attach Request. If the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the twelfth event.
frequency must be an integer from 1 to 16.

inter-rat

Enables/disables authentication for Inter-RAT Attaches.

Usage

Authentication for Attach is disabled by default. This command enables/disables authentication for an Attach with a local P-TMSI or Attaches with an IMSI, which will be authenticated to acquire the CK (cipher key) and the IK (integrity key).

Example

The following command configures authentication to occur after every tenth attach event for GPRS access.

```
authenticate attach frequency 10 access-type gprs
```

The following command disables authentication for Inter-RAT Attaches, use:

```
no authenticate attach inter-rat
```

authenticate detach

Allows the operator to enable and define authentication for Detach procedures.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
authenticate detach access-type { gprs | umts }

[ no | remove ] authenticate detach [ access-type { gprs | umts }
```

no

Disables the defined authentication procedures configured for Detach Requests from the call control profile.

remove

Deletes the defined authentication procedures for Detach Requests from the call control profile configuration file.

access-type *type*

One of the following must be selected to identify the type of network access if the **access-type** keyword is included in the command:

- **gprs**
- **umts**

Usage

Authentication for Detach procedures is disabled by default. This command enables/disables authentication for a Detach Request and allows the operator to limit authentication based on the MS/UE access-type.

Example

The following command configures detach authentication to occur only for UMTS attached subscribers:

```
authenticate detach access-type umts
```

The following command disables authentication for all Detach Requests, use:

```
no authenticate detach
```

authenticate on-first-vector

Allows the operator to enable the SGSN to begin MS authentication immediately after receiving the first vector from the HLR.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
authenticate on-first-vector

remove authenticate on-first-vector
```

remove

Removes the authenticate on-first-vector definition from the configuration file and resets the default behavior so that the SGSN waits to receive all vectors before beginning authentication towards the MS.

Usage

After an initial attach request, some end devices restart themselves after waiting for the PDP to be established. In such cases, the SGSN restarts and a large number of end devices repeat their attempts to attach. The attach requests flood the radio network, and if the devices timeout before the PDP is established then they continue to retry, thus even more traffic is generated.
To avoid the high traffic levels during PDP establishment, the SGSN has been modified to reduce the attach time, as much as possible, so that the devices can attach and discontinue sending requests. The current enhancement is intended to reduce the time needed to retrieve vectors over the GR interface by allowing the operator to configure the SGSN to start authentication towards the MS as soon as it receives the first vector from the AuC/HLR. With the new command included in the configuration, the SGSN begins the MS authentication process immediately after receiving the first vector from the HLR while the SAI continues in parallel.

Example

Use the following command to configure the SGSN to begin MS authentication immediately after receiving the first vector from the AuC/HLR:

```
authenticate on-first-vector
```

Use the following command to reset the default behavior, so that the SGSN waits to receive all vectors requested in the SAI from the AuC/HLR before begining authentication towards the MS:

```
remove authenticate on-first-vector
```

authenticate rau

Enables or disables and fine tunes authentication procedures for routing area updates (RAUs)

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

authenticate rau [access-type { gprs | umts } | frequency *frequency* **[access { gprs | umts }] | periodicity** *duration* **[access { gprs | umts }] | update-type { combined-update | imsi-combined-update | periodic | ra-update } [access-type { gprs | umts } | frequency** *frequency* **| periodicity** *duration* **| with { foreign-ptmsi | inter-rat-local-ptmsi | local-ptmsi } [access-type { gprs | umts } | frequency** *frequency* **| periodicity** *duration* **]**

no authenticate rau [access-type { grps | umts } | update-type { combined-update | imsi-combined-update | periodic | ra-update } [access-type { gprs | umts } | with { foreign-ptmsi | inter-rat-local-ptmsi | local-ptmsi } [access-type { gprs | umts }]

remove authenticate rau [access-type { gprs | umts } | periodicity [access { gprs | umts }] | update-type { combined-update | imsi-combined-update | periodic | ra-update } [access-type { gprs | umts } | periodicity | with { foreign-ptmsi | inter-rat-local-ptmsi | local-ptmsi } [access-type { gprs | umts } | periodicity]]

no

Disables authentication for the RAUs specified in the configuration for the call control profile.

remove

Deletes the authentication configuration for the RAUs from the call control profile in the configuration file.

access-type *type*

One of the following must be selected to identify the type of network access if the **access-type** keyword is included in the command:

- **gprs**
- **umts**

The **access-type** keyword can be included with any of the other keywords available with the **authenticate rau** command.

frequency *frequency*

Defines 1-in-N selective authentication for RAU events. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the twelfth event.
frequency must be an integer from 1 to 16.

periodicity *duration*

Defines the length of time (number of minutes) that authentication can be skipped.

duration: Must be an integer from 1 to 10800.

update-type

Defines the type of RAU Request. Select one of the following:

- **combined-update [access-type | with inter-rat-local-ptmsi]**
- **imsi-combined-update [access-type | with inter-rat-local-ptmsi]**
- **periodic [access-type | frequency | periodicity]**
- **ra-update [access-type | with inter-rat-local-ptmsi]**

Usage

By default, authentication is not performed for routing area updates (RAUs). Use this command to enable/disable authentication and to fine tune the authentication procedure based on frequency, periods for skipping authentication and the various types of routing area updates.

Example

The following command configures RAU authentication to occur after every tenth event for GPRS access.

```
authenticate rau frequency 10 access-type gprs
```

The following command disables authentication for RAUs based on the combined IMSI with foreign P-TMSIs, use:

```
no authenticate rau imsi-combined-update with foreign-ptmsi
```

The following command deletes all authentication configuration from the call control profile for all RAUs using GPRS access-type:

```
remove authenticate rau access-type gprs
```

authenticate service-request

Enables or disables and fine-tunes authentication procedures for Service Requests.

Product

MME, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
authenticate service-request [ frequency frequency | periodicity duration | service-type
{ data | page-response | signaling } [ frequency frequency | periodicity  duration ] ]

no authenticate service-request [ service-type { data | page-response | signaling } ]

remove authenticate service-request [ periodicity  | service-type { data | page-response
| signaling } [ periodicity ] ]
```

no

Disables authentication for the Service Requests specified in the configuration for the call control profile.

remove

Deletes the authentication configuration for Service Requests from the call control profile in the configuration file.

frequency *frequency*

Defines 1-in-N selective authentication for this type of subscriber event - Service Request. If the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the twelfth event.
frequency must be an integer from 1 to 16.

periodicity *duration*

Defines the length of time (number of minutes) that authentication can be skipped.
duration: Must be an integer from 1 to 10800.

signaling-type

Defines the type of service being requested by the Service Request. Select one of the following:

- **data**
- **page-response**
- **signaling**

Usage

By default, authentication is not performed for Service Requests. Use this command to enable/disable authentication and to fine-tune the authentication procedure based on frequency and periods for skipping authentication and the various types of service. Repeat the commands as needed to configure criteria for all service types.

Example

The following command configures authentication Service Requests for data service to only occur every 5 minutes:

```
authenticate service-request service-type data periodicity 5
```

authenticate sms

Enables or disables and fine tunes authentication procedures for Short Message Service (SMS).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

authenticate sms [access-type { gprs | umts } | frequency *frequency* **[access-type { gprs umts }] | sms-type { mo-sms | mt-sms } [access-type { gprs | umts } | frequency** *frequency* **]]**

[no | remove] authenticate sms [access-type { gprs | umts } | sms-type { mo-sms | mt-sms } [access-type { gprs umts }]]

no

Disables authentication for the SMS Requests specified in the configuration for the call control profile.

remove

Deletes the authentication configuration for SMS Requests from the call control profile in the configuration file.

access-type *type*

One of the following must be selected to identify the type of network access if the **access-type** keyword is included in the command:

- **gprs**
- **umts**

The **access-type** keyword can be included with any of the other keywords available with the **authenticate sms** command.

frequency *frequency*

Defines 1-in-N selective authentication for SMS Requests. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the twelfth event.
frequency must be an integer from 1 to 16.

sms-type

Enables authentication for the following SMS types:

- **mo-sms**: mobile-originated SMS
- **mt-sms**: mobile-terminated SMS

Usage

By default, authentication is not performed for short message service (SMS). Use this command to enable/disable authentication and to fine-tune the authentication procedure based on MS/UE access type and

the frequency for the selected SMS type. Repeat the commands as needed to configure criteria for all service types.

Example

The following command configures MO-SMS authentication to occur every fifth request:

```
authenticate sms sms-type mo-sms frequency 5
```

authenticate tau

Allows the operator to enable/disable and fine-tune authentication for the tracking area update (TAU) procedures.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

authenticate tau [freqency *frequency* **| inter-rat | periodicity** *interval* **]**

no authenticate tau inter-rat

no

Disables the TAU authentication procedures specified in the call control profile configuration.

frequency *frequency*

Defines 1-in-N selective authentication for this type of subscriber event - a tracking area update for an inter-RAT Attach. If the frequency is set for 12, the MME skips authentication for the first 11 events and authenticates on the twelfth event.
frequency must be an integer from 1 to 16.

inter-rat

Enables authentication for TAU procedures for inter-RAT Attaches.

periodicity *duration*

Defines the length of time (number of minutes) that authentication can be skipped.
duration: Must be an integer from 1 to 10800.

Usage

Authentication for TAU procedures is disabled by default. This command enables/disables authentication for a inter-RAT TAU procedures and allows the operator to limit authentication based on the frequency of the events or elapsed intervals between the events.

Example

The following command configures TAU authentication to occur when there is 15 minutes between inter-RAT Attaches:

```
authenticate tau periodicity 15
```

The following command disables authentication for all TAU Inter-RAT Attaches, use:

```
no authenticate tau
```

cc

Defines the charging characteristics to be applied for CDR generation when the handling rules are applied via the Operator Policy feature.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
cc { behavior-bit no-records bit_value | local-value behavior bit_value profile index_bit
| prefer { hlr-hss-value | local-value } }

no cc behavior-bit no-records

remove cc { behavior-bit no-records | local-value | prefer }
```

---

no

Disables the charging characteristics configuration of behavior bit from this call control profile.

---

remove

Removes the configured charging characteristics from this profile.

---

behavior-bit no-records *bit_value*

Default: disabled
Specify the charging characteristic behavior bit. **no-records** indicates that no accounting records should be generated.
If charging characteristics has no-records bit set, the system will not generate any accounting records, regardless of what may be configured elsewhere. Use "no" to indicate that there is no such bit.
bit_value must be must be an integer from 1 through 12.

---

local-value behavior *bit_value* **profile** *index_bit*

Default: bit_value = 0x0
index_bit = 8
This keyword sets the call control profile to configure the value of the behavior bits and profile index for the charging characteristics when the HLR does not provide value for this.
If the HLR provides the charging characteristics with behavior bits and profile index and operator want to ignore it, then specify **prefer local-value** keyword with this command.
bit_value: Enter a hexadecimal value between 0x0 and 0xFFF.
index_bit: Enter an integer value from 1 through 15.
Some of the index values are predefined according to 3GPP standard:

- **1** for hot billing
- **2** for flat billing
- **4** for prepaid billing
- **8** for normal billing

prefer { hlr-hss-value | local-value }

Default: **hlr-hss-value**
Specifies preference for using charging characteristics settings received from HLR or HSS, or set by the SGSN or MME locally.

- **hlr-hss-value**: Sets the call control profile to use charging characteristics settings received from HLR or HSS. This is the default preference.
- **local-value**: Sets the call control profile to use charging characteristics settings from the SGSN or MME only. If no charging characteristics received from HLR then local value will be applicable.

Usage

Use this command to set the behavior for charging characteristic coming from either an HLR or locally from an SGSN.
These charging characteristics parameters are configurable from APN Profile configuration mode too. For generation of M-CDRs, the parameters configured in this mode, Call Control Profile configuration mode, will prevail but for generation of S-CDRs the parameters configured in the APN Profile configuration mode will prevail.
The first four bits of charging characteristics (use keyword profile) is for the charging trigger profile index and is used to select different charging trigger profiles.
The 12 behavior bits (with keyword local-value behavior) can to enable or disable the CDR generation.

Example

The following command specifies a rule not to use records for charging characteristics and to set behavior bit to *2*:

```
cc behavior-bit no-records 2
```

check-zone-code

Enables or disables the zone code checking mechanism.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | remove ] check-zone-code
```

no

Included with the command, this keyword disables the mechanism.

remove

Included with the command, this keyword causes the removal of the current **check-zone-code** configuration and returns to the SGSN to the default where zone-code checking is enabled.

Usage

Use this command to enable/disable the zone-code checking function.

Example

Disable checking of the zone code:

```
no check-zone-code
```

ciphering-algorithm-gprs

Defines the order of preference of the ciphering algorithms.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ciphering-algorithm-gprs priority *priority algorithm*

remove ciphering-algorithm-gprs priority *priority*

remove

Delete the priority definition.

priority *priority*

Sets the order in which the algorithm will be selected for use.
priority is an integer from 1 to 8.

algorithm

Identifies the ciphering algorithm to be used.
algorithm is one of the following: `gea0, gea1, gea2, gea3.`

Usage

Define the order in which the ciphering algorithms are chosen for use. The command can be repeated to provide multiple definitions -- multiple priorities.

Example

Define gea1 as the third priority algorithm:

```
ciphering-algorithm-gprs priority 3 gea1
```

csfb

Configures circuit-switched fallback options. CSFB is the mechanism to move a subscriber from LTE to a legacy technology to obtain circuit switched voice or short message.

Product

MME

Privilege

Administrator

Syntax

```
csfb { policy { not-allowed | sms-only } | sms-only }

remove csfb { policy | sms-only }
```

remove csfb { policy | sms-only }

sms-only: Removes the SMS-only restriction allowing the UE to request voice and short message service (SMS) support for circuit-switched fallback (CSFB).
policy: Removes the configured policy

policy { not-allowed | sms-only }

not-allowed: Specifies that the CSFB function is not allowed for both voice and SMS.
sms-only: Specifies that the CSFB function only supports SMS.

sms-only

Specifies that the circuit-switched fallback function only supports SMS.

Important: This is a legacy keyword that remains to support earlier versions of the code. It operates identically to the **policy sms-only** keyword.

Usage

Use this command to restrict the circuit-switched fallback function to SMS only or no support for either voice or SMS.

Example

The following command enforces the SMS-only functionality for UEs requesting circuit-switched fallback:

```
csfb policy sms-only
```

description

Allows you to enter a relevant descriptive string.

Product

MME, SGSN, S-GW

Privilege

Security Administrator, Administrator

Syntax

description *description*

no description

description

Enter an alphanumeric string of 1 to 100 characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotation marks (“).

no

Removes the description from the call control profile.

Usage

Define information that identifies this particularly call control profile.

Example

```
description “call-control-profile handling incoming from CallTell”
```

diameter-result-code-mapping

Maps an EMM (EPS Mobility Management) NAS (Network Access Server) cause code to map to a Diameter result code.

Product

MME

Privilege

Administrator

Syntax

```
diameter-result-code-mapping s6a diameter-error-rat-not-allowed mme-emm-cause { no-suitable-cell-in-tracking-area | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

remove diameter-result-code-mapping s6a diameter-error-rat-not-allowed
```

`remove diameter-result-code-mapping s6a diameter-error-rat-not-allowed`

Removes the mapping.

`s6a diameter-error-rat-not-allowed`

Specifies the Diameter result code to which the EMM NAS cause code is mapped.

`mme-emm-cause { no-suitable-cell-in-tracking-area | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }`

Specifies the EMM NAS cause mapped to the Diameter result code.
`no-suitable-cell-in-tracking-area`: Specifies that the EMM NAS cause code “no suitable cell in tracking area” is to be mapped to the specified Diameter result code.
`roaming-not-allowed-in-this-tracking-area`: Specifies that the EMM NAS cause code “roaming not allowed in this tracking area” is to be mapped to the specified Diameter result code.
`tracking-area-not-allowed`: Specifies that the EMM NAS cause code “tracking area not allowed” is to be mapped to the specified Diameter result code.

Usage

Use this command to map a selected EMM NAS cause code to a specific Diameter result code.

Example

The following command maps the EMM NAS cause code “roaming not allowed in this tracking area” to the Diameter result code “S6a Diameter error RAT not allowed”:

```
diameter-result-code-mapping s6a diameter-error-rat-not-allowed mme-emm-cause roaming-not-allowed-in-this-tracking-area
```

direct-tunnel

Allows direct tunneling if direct tunneling is supported by the destination node.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
direct-tunnel attempt-when-permitted

remove direct-tunnel
```

remove

Removes the configured setting from the call control profile.

attempt-when-permitted

Enables direct tunneling if the destination node allows it. Default: disabled.

Usage

Use this command to enable the Direct-Tunnel feature.
To ensure that direct tunnel is fully configured for support by the SGSN, check the settings for **direct-tunnel** in

- the APN profile -- from the Exec mode, use command: **show apn-profile** *<profile_name>* **all**
- the RNC (radio network controller) configuration -- from the Exec mode, use command: **iups-service** *<service_name>* **all**

Important: Direct tunneling must be enabled at both of these two points to allow direct tunneling for the MS/UE.

Example

The following command sets the configuration to instruct the SGSN to attempt to setup a direct tunnel if permitted at the destination node:

```
direct-tunnel attempt-when-permitted
```

dns-ggsn

Defines the context to be used to do DNS lookup for GGSNs.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

dns-ggsn context *ctxt_name*

no dns-ggsn context *ctxt_name*

no

Removes the dns-ggsn configuration from this call control profile.

context *ctxt_name*

Specifies the context to be used to do DNS lookup for GGSNs as an alphanumeric string of 1 through 64 characters.

Usage

Use this command to define the context to be used to do DNS lookup to find the GGSN address.

Example

```
dns-ggsn context sgsn1
```

dns-sgsn

Identifies the context to be used to do DNS to find an SGSN address.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] dns-sgsn context *ctxt_name*

no

Removes the dns-sgsn configuration from this call control profile.

context *ctxt_name*

Specifies the context to be used to do DNS to find an SGSN address as an alphanumeric string of 1 through 64 characters.

Usage

Use this command to configure the context ID for the SGSN address that will be used to do the DNS lookup.

Example

```
dns-sgsn context sgsn1
```

dns-pgw

Defines the context to be used to do DNS lookup for P-GWs.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

[remove] dns-pgw context *ctxt_name*

remove

Deletes this definition from the call control profile.

context *ctxt_name*

Specifies the context to be used to do DNS lookup for P-GWs as an alphanumeric string of 1 through 64 characters.

Usage

Use this command to configure the context ID for the DNS lookup.

Example

```
dns-pgw context pgw1
```

dns-sgw

Defines the context to be used to do DNS lookup for S-GWs.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

[remove] dns-sgw context *ctxt_name*

remove

Deletes this definition from the call control profile.

context *ctxt_name*

Specifies the context to be used to do DNS lookup for S-GWs as an alphanumeric string of 1 through 64 characters.

Usage

Use this command to configure the context ID for the DNS lookup.

Example

```
dns-sgw context sgw1
```

encryption-algorithm-lte

Defines the priorities for using the encryption algorithms.

Product

MME

Privilege

Administrator

Syntax

```
encryption-algorithm-lte priority1 128-eea { 0 | 1 | 2 } priority2 128-eea { 0 | 1 | 2 }
priority3 128-eea { 0 | 1 | 2 }

remove encryption-algorithm-lte
```

remove

Deletes the priorities definition from the call control profile configuration.

priority1 128-eea { 0 | 1 | 2 }

Enter 0, 1, or 2 at the end of **128-eea** to define the algorithm being given first priority.

priority2 128-eea { 0 | 1 | 2 }

Enter 0, 1, or 2 at the end of **128-eea** to define the algorithm being given second priority.

priority3 128-eea { 0 | 1 | 2 }

Enter 0, 1, or 2 at the end of **128-eea** to define the algorithm being given third priority.

Usage

Set the order or priority in which the MME will select a 128-EEA algorithm for use. All three priorities must be set or the definition is invalid. The command can be re-entered to change the priorities without removing the configuration.

Example

Configure 128-EEA2 as first priority encryption algorithm:

```
encryption-algorithm-lte priority1 128-eea 2 priority2 128-eea 0
priority3 128-eea 1
```

encryption-algorithm-umts

Defines the priorities for using the encryption algorithms.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

encryption-algorithm-umts { *uea0* | *uea1* | *uea2* } [then-uea*#* | then-uea*#*]

no encryption-algorithm-lte

no

Deletes the priorities definition from the call control profile configuration.

{ *uea0* | *uea1* | *uea2* }

Enter one of the three options to define the first priority algorithm.

[then-uea# | then-uea#]

If a second algorithm is to be included as an option, give it second priority. Enter 0, 1, or 2 at the end of **then-uea** to define the algorithm being given second priority.

then-uea#

If a third algorithm is to be included as an option, give it third priority. Enter 0, 1, or 2 at the end of **then-uea** to define the algorithm being given third priority.

Usage

Set the order or priority in which the SGSN will select a UEA algorithm for use. It is not necessary to define priorities for all three priority levels. The command can be re-entered to change the priorities without removing the configuration.

Example

Configure algorithm UEA2 as the first priority encryption algorithm with no others to be considered:

```
encryption-algorithm-umts uea2
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

equivalent-plmn

Configures the definition for an equivalent public land mobile network identifier (PLMN ID) and the preferred radio access technology (RAT). This is a of PLMNs which should be considered by the mobile as equivalent to the visited PLMN for cell reselection and network selection. When configured, the equivalent PLMN list will be sent to the UE in NAS ATTACH ACCEPT / TAU ACCEPT messages (up to 15 PLMNs in each message).

Product

MME, SGSN

Privilege

Security Administrator, Administrator

Syntax

equivalent-plmn radio-access-technology { 2G | 3g | 4g | any } plmnid mcc *mcc_number* **mnc** *mnc_number* **priority** *priority*

no equivalent-plmn radio-access-technology { 2G | 3g | any } plmnid mcc*mcc_number* **mnc** *mnc_number*

no

Removes the equivalent-PLMN configuration from this call control profile.

radio-access-technology { 2G | 3g | 4g | any }

Identify the RAT type of the equivalent PLMN:

- **2G**: 2nd generation
- **3G**: 3rd generation
- **4G**: 4th generation
- **any**: Any RAT

plmnid mcc *mcc_number* **mnc** *mnc_number*

- **mcc**: Specifies the mobile country code (MCC) portion of the PLMN ID. The number can be any integer between 100 and 999.
- **mnc**: Specifies the mobile network code (MNC) portion of the PLMN ID. The number can be any 2- or 3-digit integer between 00 and 999.

priority *priority*

Enter an integer between 1 and 15 with the highest priority assigned to the integer of the lowest numeric value.

Usage

Use the command to identify an ‘equivalent PLMN’ and assign it a priority to define the preferred equivalent PLMN to be used. This command can be entered multiple times to set priorities of usage.

Example

The following command sets up a secondary equivalent PLMN definition that allows for any RAT with a PLMN ID of MCC121.MNC767:

```
equivalent-plmn radio_access_technology any plmnid mcc 121 mnc 767
priority 2
```

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

gmm information-in-messages

Provides the configuration to include the information in messages for the GPRS mobility management (GMM) parameters.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gmm information-in-messages access-type { { gprs | umts } [network-name { full-text *name* **| short-text** *name* **} | [send-after { attach | rau }] }**

[default | no] gmm { information-in-messages access-type { gprs | umts }

---

no

Disables the GMM configuration from this call control profile.

---

default

Sets up a GMM configuration with system default values.

---

access-type

Must select one of the following options:

- **gprs** - General Packet Radio Service network
- **umts** - Universal Mobile Telecommunications System network

After selecting the access-type, an additional parameter can be configured:

- **network-name**: identifies the network name in either short text or full text.
- **send-after**: configures the information in message to send after attachment or Routing Area Update (RAU).

---

network-name { full-text *name* **| short-text** *name* **}**

This keyword provides the option to add the network name to the message. The network name will in full text or short text. Possible options are:

- full-text *name*: Indicate the network name in full text
- short-text *name*: Indicate the network name in short text

---

send-after{ attach | rau }

This keyword configures the information in message to send after attachment or RAU message. Possible options are:

- **attach**: Information sent after attachment
- **rau**: Information sent after routing area update

Usage

Use this command to configure identifying information about the network that will be included in GMM messages.

Example

```
default gmm information-in-messages access-type gprs
```

gmm retrieve-equipment-identity

Configures the International Mobile Equipment Identity (IMEI) or software version (SV) retrieval and validation procedure.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gmm retrieve-equipment-identity { imei | imeisv [ unciphered ] [ then-imei ] } [ verify-
equipment-identity [ deny-greylisted ] ]

[ no | default ] gmm retrieve-equipment-identity
```

---

no

Disables the equipment identity retrieval procedure configured for this call control profile.

---

default

Sets the default action for equipment identity retrieval (EIR) procedure:

- **retrieve-equipment-identity**: Default action is disabled - no retrieval of IMEI/IMEI-SV
- **verify-equipment-identity**: Default action is disabled - no verification with Equipment Identity Register (EIR)

---

equipment-identity-type

Default: disabled
Indicates the type of equipment identification, with the possible values:

- **imei**: International Mobile Equipment Identity
- **imeisv**: International Mobile Equipment Identity - Software Version

---

imei

Indicates the equipment identity retrieval type to International Mobile Equipment Identity (IMEI). IMEI is a unique 15-digit number consisting of a TAC (Technical Approval Code), a FAC (Final Assembly Code), an SNR (Serial Number), and a check digit.

---

imeisv [unciphered] [then-imei]

Indicates the equipment identity retrieval type to IMEI with software version (SV). IMEI with SV is a unique 16-digit number consisting of a TAC (Technical Approval Code), a FAC (Final Assembly Code), an SNR (Serial Number), and a 2-digit software version number.

- **unciphered**: This optional keyword enables the unciphered retrieval of IMEI-SV. If this option is enabled the retrieval procedure will get IMEISV (if auth is still pending, get as part of Authentication and Ciphering Response otherwise, via explicit Identification Request after Security Mode Complete).
- **then-imei**: This optional keyword enables the retrieval of software version number before the IMEI. If this option is enabled the equipment identity retrieval procedure will get IMEISV on secured link

(after Security mode procedure via explicit GMM Identification Request), and if MS is not having IMEISV (responded with NO Identity), SGSN will try to get IMEI.

If no other keyword is provided, imeisv will get IMEISV on a secured link (after a Security mode procedure via explicit GMM Identification Request).

verify-equipment-identity [deny-greylisted]

Default: disabled

This keyword enables the equipment identity validation and validates the equipment identity against the EIR.

- **deny-greylisted**: This keyword fine-tunes the configuration and enables the restriction to the user having mobile equipment with an IMEI in the EIR grey list.

Usage

Use this command to enable and configure the procedures for mobile equipment identity retrieval and validation from the EIR identified in the MAP Service Configuration mode.

Example

The following command enables the SGSN to send "check IMEI" messages to the EIR:

```
gmm retrieve-equipment-identity imei verify-equipment-identity
```

gs-service

Associates the context of a Gs service interface with this call control profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gs-service *gs_srvc_name* **context** *ctx_name*

no gs-service *svc_name*

no

Removes/disassociates the named Gs service from the call control profile.

gs-service *gs_srvc_name*

Specifies the name of a specific Gs service for which to display information. *gs_srvc_name* is the name of a configured Gs service expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

context *ctx_name*

Specifies the specific context name where Gs service is configured. If this keyword is omitted, the named Gs service must exist in the same context as the GPRS/SGSN service.
ctx_name is name of the configured context of Gs service expressed as an alphanumeric string from 1 through 63 characters that is case sensitive.

Usage

Use this command to associate a specific Gs service interface with this GPRS service instance.

Important: A Gs service can be used with multiple SGSN and/or GPRS service.

Example

The following command associates a Gs service instance named *stargs1*, which is configured in context named *star_ctx*, with a call control profile:

```
gs-service stargs1 context star_ctx
```

gtp send

Configures which information elements (IE) the SGSN sends in GTP messages. These are required by the GGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtp send { imeisv [ derive-imeisv-from-imei ] | ms-timezone | rai | rat | uli }

remove gtp send { imeisv | ms-timezone | rai | rat | uli }

no gtp send
```

remove

Removes the specified GTP send definition from the system configuration.

no

Disables the specified GTP send configuration.

imeisv

Instructs the SGSN to include the IMEISV (International Mobile Equipment Identity with Software Version) of the mobile when sending GTP messages of the type Create PDP Context Request.

derive-imeisv-from-imei

This is a filter for the **imeisv** keyword. It allows the operator to configure the SGSN to send IMEI to the GGSN as IMEI-SV.
This filter instructs the SGSN to add four 1s (1111) to the final semi-octet of the CPCQ (Create PDP Context Request) message which enables the SGSN to deduce the IMEI-SV value from the IMEI. If this filter is used, then IMEI is also sent as IMEI-SV when the **gmm retrieve-equipment-identity** command is configured.

ms-timezone

Instructs the SGSN to include this IE in GTP messages of the type Create PDP Request and Update PDP Context Request. This IE specifies the offset between universal time and local time, where the MS currently resides, in 15-minute steps.
This IE is sent by default.

rai

Configures the SGSN to include the Routing Area Identity (RAI) of the SGSN in the following situations:

- 2G new SGSN RAU
- 3G new SGSN SRNS
- 2G -> 3G HO (only if PLMN Id has changed)
- 3G -> 2G HO (only if PLMN Id has changed)

- multiple IUPS service RAU (only if PLMN Id has changed)
- multiple GPRS service RAU (only if PLMN Id has changed)
- 3G new SGSN RAU (change in behavior)
- 3G primary and secondary PDP activation (change in behavior)
- 2G primary and secondary PDP activation (change in behavior)

rat

Specifies which radio access technology (RAT) is being used by the MS (GERAN, UTRAN, or GAN). Including this keyword instructs the SGSN to include this IE when sending GTP messages of the type Create PDP Request and Update PDP Context Request.
This IE is sent by default.

uli

Specifies the CGI (MCC, MNC, etc.) and SAI of the MS where it is registered. Including this keyword instructs the SGSN to include the IE when sending GTP messages of the type Create PDP Request and Update PDP Context Request.
This IE is not sent by default.

Usage

Use this command to define a preferred set of information to include when GTP messages are sent. Repeat this command multiple times to enable or disable multiple options. This instruction will be implemented when the specific operator policy and call control profile are applied.

Example

The following command series instructs the SGSN to send ULI and RAT in the GTP messages:

```
gtp send uligtp send rat
```

gtpu fast-path

Enables or disables the network processing unit (NPU) Fast Path support for NPU processing of GTP-U packets of user sessions at the NPU.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ remove ] gtpu fast-path
```

remove

Removes the NPU fast path functionality configuration from the call control profile.

Usage

Use this command to enable/disable the NPU processed fast-path feature for processing of GTP-U data packets received from GGSN/RNC. This feature enhances the GTP-U packet processing by adding the ability to fully process and forward the packets through the NPU itself.

Important: When enabled/disabled, fast-path processing will be applicable only to new subscriber who establishes a PDP context after issuing this command (enabling GTP-U fast path). No existing subscriber session will be affected by this command.

Example

The following command enables the NPU fast path processing for all new subscribers' session established with this call control profile:

```
gtpu fast-path
```

gw-selection

Configures the parameters controlling the gateway selection process.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

```
[ remove ] gw-selection { co-location | pgw weight | sgw weight | topology }
```

remove gw-selection

Deletes the gw-selection definition from the call control profile.

co-location

Selects “co-location” as the determining factor for gateway selection.

pgw weight

Selects PDN-Gateway as the determining factor for gateway selection.

sgw weight

Selects Serving Gateway as the determining factor for gateway selection.

topology

Selects topology as the determining factor for gateway selection.

Usage

Use this command to define the criteria for gateway selection.

Example

The following command instructs the MME to determine gateway selection on the basis of topology:

```
gw-selection topology
```

integrity-algorithm-lte

Specifies the order of preference for using an Integrity Algorithm.

Product

MME

Privilege

Administrator

Syntax

```
integrity-algorithm-lte priority1 { 128-eia0 | 128-eia1 | 128-eia2 } priority2 128-eia {
0 | 1 | 2 } priority3 128-eia { 0 | 1 | 2 }

remove integrity-algorithm-lte
```

remove

Deletes the priorities definition from the call control profile configuration.

priority1 128-eia { 0 | 1 | 2 }

Enter 0, 1, or 2 at the end of **128-eia** to define the algorithm being given first priority.

priority2 128-eia { 0 | 1 | 2 }

Enter 0, 1, or 2 at the end of **128-eia** to define the algorithm being given second priority.

priority3 128-eia { 0 | 1 | 2 }

Enter 0, 1, or 2 at the end of **128-eia** to define the algorithm being given third priority.

Usage

Set the order or priority in which the MME will select an integrity algorithm for use. All three priorities must be set or the definition is invalid. The command can be re-entered to change the priorities without removing the configuration.

Example

Configure 128-EIA0 as first priority integrity algorithm:

```
integrity-algorithm-lte priority1 128-eia 0 priority2 128-eia 2 priority3
128-eia 1
```

integrity-algorithm-umts

Configures the order of preference for the Integrity Algorithm used for 3G.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

integrity-algorithm-umts *type* **then_** *type*

default integrity-algorithm-umts

default

Specifies the default preference based on system defaults.

type

Creates a configuration defining an order of preference. Enter one or more of the following options in the order of preference:

- **uia1** - uia1 Algorithm
- **uia2** - uia2 Algorithm

Usage

Use this command to determine which integrity algorithm is preferred 3G. This command is configured in tandem with the algorithm type for **encryption-algorithm-umts** command.

Example

```
default integrity-algorithm-umts
```

local-cause-code-mapping

Maps a selected cause code to the restricted zone code result.

Product

MME

Privilege

Administrator

Syntax

```
local-cause-code-mapping restricted-zone-code emm-cause-code { eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

remove local-cause-code-mapping restricted-zone-code
```

remove

Removes the configured cause code mapping.

restricted-zone-code

Specifies the event for which the cause code is returned.

emm-cause-code { eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to apply when a UE requests access to a restricted zone:

eps-service-not-allowed-in-this-plmn
no-suitable-cell-in-tracking-area
plmn-not-allowed
roaming-not-allowed-in-this-tracking-area
tracking-area-not-allowed

Usage

Use this command to configure the cause code returned when a UE requests access to a restricted zone.

Example

The following command maps the “PLMN not allowed” cause code to the restricted zone code event:

```
local-cause-code-mapping restricted-zone-code emm-cause-code plmn-not-allowed
```

location-area-list

Defines the location area list to allow or restrict services in the specified location areas identified by location area code (LAC).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

location-area-list instance *instance* **area-code** *area_code* **[** *area_code* ***** **]**

no location-area-list instance *instance***[area-code** *area_code* **]**

no

If the **area-code** keyword is included in the command, then only the specified area code is removed from the identified list. If the **area-code** keyword is not included with the command, the entire list of LACs is removed from this call control profile.

instance *instance*

Specifies an identification for the specific location area list.
instance must be an integer between 1 and 5.

area-code *area_code* *****

This keyword defines the location area codes (LACs) to be used by this call control profile as a determining factor in the handling of incoming calls. Multiple LACs can be defined in a single location-area-list.
area_code: Enter an integer between 1 and 65535.
***** If desired, enter multiple LACs separated by a single blank space.

Usage

Use the command multiple times to configure multiple LAC lists or to modify the a list.

Example

The following command creates a location area list for a single area code:

```
location-area-list instance 1 area-code 514
```

This command creates a second location area list for with multiple area codes - all separated by a single blank space:

```
location-area-list instance 2 area-code 514 62552 32 1513
```

The next command corrects an area code mistake (327 not 32) made in the previous configuration:

```
location-area-list instance 1 area-code 514 62552 327 1513
```

lte-zone-code

Configures the enforcement of allowed or restricted zone code lists and associates an EPS Mobility Management (EMM) cause code to rejected attach attempts.

Product

MME

Privilege

Administrator

Syntax

```
lte-zone-code [ allow | restrict } { emm-cause-code { eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed ] zone-code-list zc_id +

remove lte-zone-code zone-code-list
```

remove

Removes the zone code list from the call control profile.

[allow | restrict]

Specifies whether the zone code list is allowed or restricted.

Important: You can only create an allowed or restricted list, not both.

emm-cause-code [eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed]

Optionally, specify one of the following EMM cause codes to apply when a UE request is rejected:
eps-service-not-allowed-in-this-plmn
no-suitable-cell-in-tracking-area
plmn-not-allowed
roaming-not-allowed-in-this-tracking-area
tracking-area-not-allowed

zone-code-list *zc_id* **+**

Specifies the zone code in the allowed or restricted list of zone codes. *zone_code* must be an integer value from 0 to 65535.

Usage

Use this command to create zone code lists that allow or restrict access to UEs managed by this call control profile.

Example

The following command restricts access to zone codes 234 and 456 and returns an EMM cause code of "tracking area not allowed":

```
lte-zone-code restrict emm-cause-code tracking-area-not-allowed zone-
code-list 234 456
```

map

Configures the optional extensions to Mobile Application Part (MAP) messages.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ remove ] map message update-gprs-location [ imeisv | private-extension access-type ]
```

remove

IMEI-SV is not included in the GLU request -- this is the default behavior.

message update-gprs-location

Includes a GLU message. This keyword-set is required.

imeisv

Specifies the International Mobile equipment Identity-Software Version (IMEI-SV) information to include in the GPRS Location Update (GLU) request message. SGSN will include IMEI-SV in the message, if available. Default: disabled

private-extension access-type

Includes a specific access-type private extension in the message.

Usage

This command configures optional extensions to MAP messages. The HLR should ignore these extensions if not supported by the HLR.

Example

```
map message update-gprs-location private-extension access-type
```

map-service

Identifies a Mobile Application Part (MAP) service and the context which contains it and associates both with the call control profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

map-service context *ctxt_name* **service** *map_srvc_name*

no map-service context

no

Disables use of MAP service with this call control profile.

context *ctxt_name*

Specifies the name of the context for the MAP service as an alphanumeric string of 1 through 64 characters.

service *map_srvc_name*

Specifies the MAP service name as an alphanumeric string of 1 through 64 characters.

Usage

Use this command to enable or disable MAP service with this call control profile.

Example

```
no map-service context
```

max-bearers-per-subscriber

Defines the maximum number of bearers allowed per subscriber.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

max-bearers-per-subscriber *number*

remove max-bearers-per-subscriber

remove

Deletes the definition from the call control profile.

number

Identifies the maximum number of bearers allowed per subscriber as an integer from 1 to 11.

Usage

Use this command to set the maximum number of bearers allowed per subscriber.

Example

Set the maximum to 3:

```
max-bearers-per-subscriber 3
```

max-pdns-per-subscriber

Defines the maximum number of PDNs allowed per subscriber.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

max-pdns-per-subscriber *number*

remove max-pdns-per-subscriber

remove

Deletes the definition from the call control profile.

number

Identifies the maximum number of PDNs allowed per subscriber as an integer from 1 to 11.

Usage

Use this command to set the maximum number of PDNs allowed per subscriber.

Example

Set the maximum to 4:

```
max-pdns-per-subscriber 4
```

min-unused-auth-vectors

Configures a specific minimum number of unused vectors to be maintained by the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

min-unused-auth-vectors *min#_vectors*

remove min-unused-auth-vectors

remove

Removes the definition from the configuration file and restores the default behavior, which does not use the threshold.

min#_vectors

Enables and defines a threshold for the minimum number of unused vectors that the SGSN retains to trigger the initation of a service area identity request (SAI) .
min#_vectors: Enter a digit betwen 1 and 4.

Usage

Vectors are used by the SGSN for authentication. Use this command to enable a minimum threshold for unused vector for this call control profile. When the unused vector count falls below this configured threshold, then an SAI is initiated to fill the buffer back to 5 or to the most appropriate number based on the MAP service configuration.

Example

Enter a command similar to the following to set a threshold of *3*:

```
min-unused-auth-vectors 3
```

Use the following command to disable this function and restore the default behavior, which does not use a threshold to trigger an SAI:

```
remove min-unused-auth-vectors
```

network-feature-support-ie

Configures support for IMS Voice over Packet-Switched information element (IE) as part of the MME (Network) Feature Support.

Product

MME

Privilege

Administrator

Syntax

```
network-feature-support-ie ims-voice-over-ps

remove network-feature-support-ie
```

remove

Disables support for Voice over PS.

ims-voice-over-ps

Enables support for Voice over PS.

Usage

Use this command to enable Voice over PS which "switches on" an IE in a message sent by the MME indicating the features it supports.

Example

The following command enables Voice over PS on the MME:

```
network-feature-support-ie ims-voice-over-ps
```

network-initiated-pdp-activation

Configures the call control profile to perform two functions: (1) to enable or disable network-requested PDP context activation (NRPCA) for 3G attachments and (2) to define a failure cause code for inclusion in NRPCA-related reject messages.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

`[ remove ] network-initiated-pdp-activation { allow primary | restrict primary } access type { gprs | umts } { all | location-area-list instance` *`<instance>`* **`}`**

`network-initiated-pdp-activation primary access type { gprs | umts } { all | location-area-list instance` *`<instance>`* **`} failure-code`***`code`*

`remove`

Including this keyword with the command, removes all configured values for the specified configuration.

`allow`

Allows network-initiated PDP context activation. This keyword must be followed by other parameters to indicate the limitations for allowing the NRPCA.
Allow is the default for NRPCA.

`restrict`

Restricts network-initiated PDP context activation. This keyword must be followed by other command parameters to indicate the limitations for restricting the NRPCA.

`primary`

Specifies that only network-initiated primary PDP context activations are to be allowed.

`secondary`

Important: The **`secondary`** keyword is visible and can be selected, however, secondary NRPCA functionality is in development and currently this keyword is not supported for configuration.

`all`

Configures the SGSN to allow or to restrict NRPCA for calls within all location areas.

`location-area-list instance` *`instance`*

Selects a pre-defined list of location area codes (LACs) and allows/restricts the NRPCA procedure for calls within the listed area codes.
`instance`: Enter a list ID; an integer between 1 and 5.

Important: Before using this keyword, ensure that the appropriate LAC information has been defined with the **location-area-list** command, also in this configuration mode.

failure-codes *code*

Enter an integer from 192 to 226 to identify the GTPP failure cause code (from 3GPP TS29.060, list below) to be included in the reject messages when NRPCA is restricted. If a failure cause code is not defined, the default value is 200 (service not supported).

- 192 - Non-existent
- 193 - Invalid message format
- 194 - IMSI not known
- 195 - MS is GPRS Detached
- 196 - MS is not GPRS Responding
- 197 - MS Refuses
- 198 - Version not supported
- 199 - No resources available
- 200 - Service not supported
- 201 - Mandatory IE incorrect
- 202 - Mandatory IE missing
- 203 - Optional IE incorrect
- 204 - System failure
- 205 - Roaming restriction
- 206 - P-TMSI Signature mismatch
- 207 - GPRS connection suspended
- 208 - Authentication failure
- 209 - User authentication failed
- 210 - Context not found
- 211 - All dynamic PDP addresses are occupied
- 212 - No memory is available
- 213 - Relocation failure
- 214 - Unknown mandatory extension header
- 215 - Semantic error in the TFT operation
- 216 - Syntactic error in the TFT operation
- 217 - Semantic errors in packet filter(s)
- 218 - Syntactic errors in packet filter(s)
- 219 - Missing or unknown APN
- 220 - Unknown PDP address or PDP type
- 221 - PDP context without TFT already activated
- 222 - APN access denied – no subscription

- 223 - APN Restriction type incompatibility with currently active PDP Contexts
- 224 - MS MBMS Capabilities Insufficient
- 225 - Invalid Correlation-ID
- 226 - MBMS Bearer Context Superseded

Usage

Use this command to allow or restrict network-requested PDP context activation (NRPCA) based on access-type and location areas. NRPCA is used when there is downlink data at the GGSN for a subscriber, but there is no valid context for the already-established PDP address so the GGSN initiates an NRPCA procedure towards the SGSN.

This command can also be used to define the failure cause code that will be included in activation reject messages.

These commands can be repeated to define a unique set of NRPCA parameters for each access-type and each location area list.

The **T3385-timeout** and the **max-actv-retransmission** timers configure the retransmission timer and the number of retries for PDP context activation requests. Both of these timers are set in the SGSN service configuration mode.

The configuration for NRPCA can be viewed via the **show call-control-profile full name** *profile_name*. Statistics associated with NRPCA can be seen via the **show gmm-sm statistics** output and via the **show sgtpc statistics verbose** output.

Example

The following command changes the failure code for Reject messages from 200 (service not supported) to 205 (roaming restriction) for primary NRPCA for all GRPS access and all LACs:

```
network-initiated-pdp-activation primary access-type gprs all failure-
code 205
```

The following command enables network-initiated primary PDP context activation for UMTS calls from the LACs in location-area-list 1:

```
network-initiated-pdp-activation allow primary access-type umts location-
area-list instance 1
```

The following command restricts network-initiated primary PDP context activation for UMTS calls from the LACs in location-area-list 2:

```
network-initiated-pdp-activation restrict primary access-type umts
location-area-list instance 2
```

override-arp-with-ggsn-arp

Enables or disables the ability of the SGSN to override an Allocation/Retention Priority (ARP) value with one received from a GGSN. If there is no authorized Evolved ARP received from the GGSN, by default the SGSN continues to use the legacy ARP included in the Quality of Service (QoS) Profile IE.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ remove ] override-arp-with-ggsn-arp
```

remove

Adding the **remove** keyword to the command disables the override feature.

Usage

Enabling this function on the SGSN will allow the ARP sent by the GGSN, in CPCR / UPCR / UPCQ, to be applicable as an overriding value.

Example

Use this command to configure the SGSN to negotiate the ARP to be used as an overriding value:

```
override-arp-with-ggsn-arp
```

pdp-activate access-type

Configures the PDP context activation option based the type of access technology.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

pdp-activate access-type { grps | umts } { all | location-area-list instance *instance* **} failure-code** *failure_code*

default pdp-activate access-type { grps | umts } { all | location-area-list instance *instance* **} failure-code** *code*

default

Resets the configuration to system default values for PDP context activation request.

{ grps | umts }

Specifies the access technology type for PDP context activation.

- **gprs**: Enables access type as GPRS.
- **umts**: Enables access type as UMTS.

all

Default: allow
Configures the system to allow the creation of all PDP context activation requests received from MS.

location-area-list instance *instance*

Specifies the location area instance for which to create a PDP context as an integer from 1 through 5. The value must be an already defined instance of a location area code (LAC) list created via the **location-area-list** command.

failure-code *code*

Specifies the failure code for PDP context activation as an integer from 8 through 112. Default: 8

Usage

Use this command to configure this call control profile to allow GPRS/UMTS access through PDP context activation request from MS.

Example

The following command configures the system to create the PDP context for requests from MS for GPRS access with location area list instance *2* and failure-code *5*:

```
pdp-activate access-type gprs location-area-list 2 failure-code 5
```

pdp-activate allow

Configures the system to allow the PDP context activation based on the type of access technology.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] pdp-activate allow access-type { grps | umts } location-area-list instance *instance*

no

Removes the configured permission to create PDP context on request of PDP context activation from MS for an access type.

access-type { grps | umts }

Specifies the access technology type for PDP context activation.

- **gprs**: Enables access type as GPRS.
- **umts**: Enables access type as UMTS.

location-area-list instance *instance*

Specifies the location area instance to create PDP context.
instance must be an integer from 1 through 5. The value must be an already defined instance of a location area code (LAC) list created via the **location-area-list** command.

Usage

Use this command to configure this call control profile to allow GPRS/UMTS access through PDP context activation request from MS.

Example

The following command configures the system to allow the PDP context activation for GPRS access type with location area list instance *2*:

```
pdp-activate allow access-type gprs location-area-list instance 2
```

pdp-activate restrict

Configures the system to restrict the PDP context activation based on the type of access technology.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] pdp-activate restrict { { access-type { grps | umts } { all | location-area-list
instance instance } | secondary-activation { access-type { grps | umts } { all |
location-area-list instance instance } } }
```

no

Removes the configured restriction on PDP context activation through this command.

access-type { grps | umts }

Specifies the access technology type for which to restrict PDP context activation.

- **gprs**: Enables access type as GPRS.
- **umts**: Enables access type as UMTS.

all

Default: allow
Configures the system to restrict all PDP context activation requests from the MS.

location-area-list instance *instance*

Specifies the location area instance to restrict PDP context activation.
list_id must be an integer from 1 through 5. The value must be an already defined instance of a location area code (LAC) list created with the **location-area-list** command.

secondary-activation

Specifies the type of PDP context to restrict for secondary activation. This keyword restricts the system to create the secondary PDP context on receiving the PDP Context Activation Request from the MS.

Usage

Use this command to configure this call control profile to restrict GPRS/UMTS access through PDP context activation request from MS.

Example

The following command configures the system to restrict the PDP context activation for request from MS to access GPRS service with location area list instance *2*:

```
pdp-activate restrict access-type gprs location-area-list instance 2
```

plmn-protocol

Configures the protocol supported by the PLMN (Public Land Mobile Network).

Product

MME

Privilege

Security Administrator, Administrator

Syntax

plmn-protocol plmnid mcc *mcc_num* **mnc** *mnc_num* **{ s5-protocol | s8-protocol } { gtp | pmip }**

remove plmn-protocol plmnid mcc *mcc_num* **mnc** *mnc_num*

remove

Deletes the definition from the call control profile configuration.

plmn-id mcc *mcc_num* **mnc** *mnc_num*

Identifies the PLMN by MCC (mobile country code) and MNC (mobile network code).
mcc_num: Enter a 3-digit integer from 100-999.
mnc_num: Enter a 2- or 3-digit integer from 00 to 999.

s5-protocol | s8-protocol

Select which protocol – S5 or S8 – that controls the identified PLMN.

gtp | pmip

Select the protocol variant - GTP or PMIP - that controls functionality for the identified PLMN.

Usage

Use this command to identify a particular PLMN and, at a higher level, its operational characteristics.

Example

The following command instructs the MME to use PLMN MCC423.MNC40.GPRS with PMIP under S8 Protocol:

```
plmn-protocol plmnid mcc 423 mnc 40 s8-protocol pmip
```

ptmsi-reallocate

Defines P-TMSI reallocation for Attach Requests, RAU Request, and Service Requests.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ptmsi-reallocate { attach | frequency *frequency* **| interval** *interval* **| routing-area-update [update-type] | service-request [service-type] } [access-type { gprs | umts }]**

ptmsi-reallocate routing-area-update [access-type { gprs | umts } | frequency *frequency* **| update-type { combined-update | imsi-combined-update | periodic | ra-update } [access-type { gprs | umts } | frequency** *frequency* **]]**

ptmsi-reallocate service-request [frequency *frequency* **| service-type { data | page-response | signaling } [frequency** *frequency* **]]**

[no | remove] ptmsi-reallocate { attach | frequency | interval | routing-area-update [update-type { combined-update | imsi-combined-update | periodic | ra-update } [access-type { gprs | umts }]] | service-request [service-type { data | page-response | signaling }] } [access-type { gprs | umts }]

no

Disables the authentication procedures configured for the specified P-TMSI reallocation configuration in the call control profile.

remove

Deletes the defined authentication procedures for the specified P-TMSI reallocation configuration from the call control profile configuration file.

attach

Enables/disables P-TMSI reallocation for Attach with local P-TMSI.

Important: IMSI or inter-SGSN Attach is not configurable and will always be reallocated.

access-type *type*

One of the following must be selected to reallocate on the basis of the type of network access:

- **gprs**
- **umts**

This keyword can be used in combination with other keywords to refine the reallocation configuration.

frequency *frequency*

Defines 1-in-N selective reallocation. If the frequency is set for 12, then the SGSN skips reallocation for the first 11 messages and reallocates on receipt of the 12th request message.
frequency must be an integer from 1 to 50.
This keyword can be used in combination with other keywords to refine the reallocation configuration.

interval *minutes*

Enter an integer between 1 and 1440 to define the time interval (in minutes) for skipping the service/RAU/attach request message procedure.

routing-area-update [update-type]

Enables/disables P-TMSI reallocation for RAU (routing area update) with local P-TMSI. To refine the reallocation configuration, include one of the optional types of updates to limit reallocation:

- **combined-update**
- **imsi-combined-update**
- **periodic**
- **ra-update**

Important: Inter-SGSN RAU will always be reallocated.

service-request [service-type]

Enables/disables P-TMSI reallocation for Service Requests. To refine the Service-Request reallocation configuration, include on of the optional service-types to limit the reallocation:

- **data**
- **page-response**
- **signaling**

Usage

By default, reallocation is not enabled. Use this command to enable P-TMSI reallocation for Attach Requests, RAU Request, and Service Requests. Fine-tune the reallocation configuration according to frequency, interval, or access-type.

Example

The following command configures the SGSN to perform P-TMSI reallocation upon receiving 2G Attach Requests

```
ptmsi-reallocate attach access-type gprs
```

The following command configures the SGSN to disable all previously defined P-TMSI reallocations based on the combined criteria of interval and 3G requests:

```
no ptmsi-reallocate interval access-type umts
```

ptmsi-signature-reallocate

Enables P-TMSI signature reallocation during Attach/RAU procedures.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ptmsi-signature-reallocate { attach | frequency *frequency* **| interval** *interval* **| ptmsi-reallocation-command | routing-area-update [update-type] } [access-type { gprs | umts } | frequency** *frequency* **]**

ptmsi-signature-reallocate routing-area-update [access-type { gprs | umts } | frequency *frequency* **| update-type { combined-update | imsi-combined-update | periodic | ra-update }] [access-type { gprs | umts } | frequency** *frequency* **]**

[no | remove] ptmsi-signature-reallocate { attach | frequency | interval | routing-area-update [update-type { combined-update | imsi-combined-update | periodic | ra-update }] } [access-type { gprs | umts }]

no

Disables the authentication procedures configured for the specified P-TMSI signature reallocation configuration in the call control profile.

remove

Deletes the defined authentication procedures for the specified P-TMSI signature reallocation configuration from the call control profile configuration file.

attach

Enables/disables P-TMSI signature reallocation for Attach with local P-TMSI.

access-type *type*

One of the following must be selected to reallocate on the basis of the type of network access:

- **gprs**
- **umts**

This keyword can be used in combination with other keywords to refine the reallocation configuration.

frequency *frequency*

Defines 1-in-N selective reallocation. If the frequency is set for 12, then the SGSN skips reallocation for the first 11 messages and reallocates on receipt of the twelfth request message.
frequency must be an integer from 1 to 50.
This keyword can be used in combination with other keywords to refine the reallocation configuration.

interval *minutes*

Enter an integer between 1 and 1440 to define the time interval (in minutes) for skipping the service/RAU/attach request message procedure before performing a P-TMSI signature reallocation.

ptmsi-reallocation-command

Includes P-TMSI signature reallocation as a part of the P-TMSI reallocation configuration.

routing-area-update [update-type]

Enables/disables P-TMSI signature reallocation for RAU (routing area update) with local P-TMSI. To refine the reallocation configuration, include one of the optional types of updates to limit reallocation:

- **combined-update**
- **imsi-combined-update**
- **periodic**
- **ra-update**

Usage

By default, P-TMSI signature reallocation is disabled. This command allows the operator to configure when the P-TMSI signature is reallocated.

Example

The following command configures the SGSN to reallocate the P-TMSI signature for every third UMTS attach procedure:

```
ptmsi-signature-reallocate attach frequency 3 access-type umts
```

The following command configures the SGSN to reallocate the P-TMSI signature for every seventh GPRS periodic RAU procedure:

```
ptmsi-signature-reallocate routing-area-update uupdate-type periodic
frequency 7 access-type gprs
```

The following command removes all configuration instances for reallocating the P-TMSI signature based on intervals and UMTS access:

```
remove ptmsi-signature-reallocate interval access-type umts
```

qos

Configures the quality of service (QoS) parameters to be applied.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

```
[ remove ] qos { gn-gp | ue-ambr }

qos gn-gp { arp high-priority priority medium-priority priority | pre-emption {
capability { may-trigger-pre-emption | shall-not-trigger-pre-emption } | vulnerability {
not-pre-emptable | pre-emptable }

qos ue-ambr max-ul mbr_up max-dl mbr_dl
```

remove

Deletes the configuration from the call control profile.

gn-gp

Configures Gn-Gp pre-release 8 ARP and pre-emption parameters.

arp

Maps usage of ARP (address retention protocol) high-priority (H) and medium-priority (M):

- **high-priority** *priority*: Enter an integer from 1 to 13.
- **medium-priority** *priority*: Enter an integer from 2 to 14.

pre-emption

Defines the pre-emption/vulnerability criteria for PDP Contexts imported from SGSN on Gn/Gp:

- **capability**
  - **may-trigger-pre-emption**: PDP Contexts imported from Gn/Gp SGSN may preempt existing bearers.
  - **shall-not-trigger-pre-emption**: PDP Contexts imported from Gn/Gp SGSN shall not preempt existing bearers.
- **vulnerability**
  - **not-pre-emptable**: PDP Contexts imported from Gn/Gp SGSN are not vulnerable to pre-emption.
  - **pre-emptable**: PDP Contexts imported from Gn/Gp SGSN are vulnerable to pre-emption.

ue-ambr

Configures the aggregate maximum bit rate that will be stored on the UE (user equipment).

- **max-ul** *mbr-up*: Defines the maximum bit rate for uplink traffic.

  mbr-up: Enter a value from 0 to 1410065408.

- **max-dl** *mbr-up*: Defines the maximum bit rate for downlink traffic.

  mbr-up: Enter a value from 0 to 1410065408.

Usage

Use this command to configure the MME QoS parameters for the call control profile.

Example

```
qos gn-gp arp high-priority 2 medium-priority 3
```

rau-inter

Defines an acceptable procedure for inter-SGSN routing area updates.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

rau-inter access-type { all | location-area-list instance *instance* **} { failure-code** *fail_code* **| user-device-release { before-r99 } { failure-code** *fail_code* **| r99-or-later } { failure-code** *fail_code* **} }**

default rau-inter access-type { all | location-area-list instance *instance***} user-device-release { before-r99 failure-code | r99-or-later failure-code }**

no rau-inter { allow access-type | restrict access-type } { [all] failure-code *fail_code* **| location-area-list instance** *instance* }

default rau-inter { allow access-type | restrict access-type } { [all] failure-code *fail_code* **| location-area-list instance** *instance* **} }**

---

no

Including "no" as part of the command structure disables the values already configured for parameters specified in the command.

---

default

Resets the configuration of specified parameters to system default values.

---

allow access-type

Including this keyword-set with one of the following options, configures the SGSN to allow MS/UE with the identified access-type extension to be part of the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

---

restrict access-type

Including this keyword-set with one of the following options, configures the SGSN to restrict MS/UE with the identified access-type extension from the inter-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

---

all

all - adding this option to the keyword determines that the failure cause code will be applicable to all location areas.

location-area-list instance *instance*

list_id must be an integer between 1 and 5. The value must be an already defined instance of a location area code (LAC) list created with the **location-area-list** command.

failure-code *fail-code*

Specify a GSM Mobility Management (GMM) failure cause code to identify the reason an inter SGSN RAU does not occur. This GMM cause code will be sent in the reject message to the MS.
fail-code must be an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

user-device-release { before-r99 | r99-or-later } failure-code *code*

Default: Disabled
Enables the SGSN to reject an Inter-RAU procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber's IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile is found that relates to this Attach Request.
3. call control profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

- **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

Usage

Use this command to configure the restrictions and function of the inter-RAU procedure.

Example

```
default rau-inter allow access-type gprs location-area-list instance 1
```

rau-inter-plmn

Enables or disables restriction of all Routing Area Updates (RAUs) occurring between different PLMNs.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

rau-inter-plmn access-type { all | location-area-list instance *instance* **} { failure-code** *fail_code* **| user-device-release { before-r99 } failure-code** *fail_code* **| r99-or-later } { failure-code** *fail_code* **} }**

default rau-inter-plmn access-type { all | location-area-list instance *instance***} user-device-release { before-r99 failure-code | r99-or-later failure-code }**

[no] rau-inter-plmn { restrict | allow } access-type { gprs | umts } { all | location-area-list instance instance }

[no] rau-inter-plmn { allow access-type | restrict access-type } { [all] failure-code *fail_code* **| location-area-list instance** *instance* **}**

default rau-inter { allow access-type | restrict access-type } { [all] failure-code *fail_code* **| location-area-list instance** *instance* **} }**

no

Including "no" as part of the command structure disables the values already configured for parameters specified in the command.

default

Resets the configuration of specified parameters to system default values.

allow access-type

Including this keyword-set with one of the following options, configures the SGSN to allow MS/UE with the identified access-type extension to be part of the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

restrict access-type

Including this keyword-set with one of the following options, configures the SGSN to restrict MS/UE with the identified access-type extension from the inter-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

all

all - adding this option to the keyword determines that the failure cause code will be applicable to all location areas.

location-area-list instance *instance*

list_id must be an integer between 1 and 5. The value must be an already defined instance of a LAC list created with the **location-area-list** command.

failure-code *fail-code*

Specify a GSM Mobility Management (GMM) failure cause code to identify the reason an inter SGSN RAU does not occur. This GMM cause code will be sent in the reject message to the MS.
fail-code must be an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state

- 111 - Protocol error, unspecified

user-device-release { before-r99 | r99-or-later } failure-code *code*

Default: Disabled
Enables the SGSN to reject an Inter-RAU procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber's IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile are found that relate to this Attach Request.
3. The call control profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

- **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

Usage

Use this command to configure the restrictions and function of the inter-RAU procedure occurring across RNCs or BSSs where the PLMN changes. For example:

- inter-IuPS RAU, where the two IuPSs have different PLMNs
- inter-GPRS RAU, where the two GPRSs have different PLMNs
- inter-RAT RAU (2G > 3G), where the IuPS/GPRS services have different PLMNs
- inter-RAT-RAU (3G > 2G), where the IuPS/GPRS services have different PLMNs

Example

```
default rau-inter allow access-type gprs location-area-list instance 1
```

rau-intra

Defines an acceptable procedure for intra-SGSN Routing Area Updates (RAUs).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

rau-intra access-type { all | location-area-list instance *instance* **} { failure-code** *fail_code* **| user-device-release { before-r99 } { failure-code** *fail_code* **| r99-or-later } { failure-code** *fail_code* **} }**

default rau-intra access-type { all | location-area-list instance *instance***} user-device-release { before-r99 failure-code | r99-or-later failure-code }**

rau-intra { allow access-type | restrict access-type } { [all] failure-code *fail_code* **| location-area-list instance** *instance* **} }**

no rau-intra { allow access-type | restrict access-type } { [all] failure-code *fail_code* **| location-area-list instance** *instance* **}**

default rau-intra { allow access-type | restrict access-type } { [all] failure-code *fail_code* | location-area-list instance *instance* **} }**

---

no

Including "no" as part of the command structure disables the values already configured for parameters specified in the command.

---

default

Resets the configuration of specified parameters to system default values.

---

allow access-type

Including this keyword-set with one of the following options, configures the SGSN to allow an MS/UE with the identified access-type extension to be part of the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

---

restrict access-type

Including this keyword-set with one of the following options, configures the SGSN to restrict an MS/UE with the identified access-type extension from the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

all

all - adding this option to the keyword determines that the failure cause code will be applicable to all location areas.

location-area-list instance *instance*

list_id must be an integer between 1 and 5. The value must be an already defined instance of a location area code (LAC) list created via the **location-area-list** command.

failure-code *fail-code*

Specify a GSM Mobility Management (GMM) failure cause code to identify the reason an inter SGSN RAU does not occur. This GMM cause code will be sent in the reject message to the MS.
fail-code must be an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state

- 111 - Protocol error, unspecified

user-device-release { before-r99 | r99-or-later } failure-code *code*

Default: Disabled
Enables the SGSN to reject an Intra-RAU procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber's IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile are found that relate to this Attach Request.
3. Call control profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

- **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

Usage

Use this command to configure the restrictions and function of the intra-RAU procedure.

Example

```
default rau-intra allow access-type gprs location-area-list instance 1
```

re-authenticate

Enables or disables the re-authentication feature. This command is available in releases 8.1 and higher.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
re-authenticate [ access-type { gprs | umts } ]

remove re-authenticate
```

remove

Including this keyword with the command disables the feature. The feature is disabled by default.

access-type

Defines the type of access to be allowed or restricted.

- **gprs**
- **umts**

If this keyword is not included, then both access types are allowed by default.

Usage

Use this command to enable or disable the re-authentication feature, which instructs the SGSN to retry authentication with another RAND in situations where failure of the first authentication has occurred. To address the introduction of new SIM cards, for security reasons a systematic "last chance" authentication retry with a fresh Authentication Vector is needed, particularly in cases where there is an SRES mismatch at authentication.

Example

```
re-authenticate
```

regional-subscription-restriction

Allows the operator to define the cause code for subscriber rejection when it is due to regional subscription information failure.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

`[ remove ] regional-subscription-restriction [ failure-code` *`code`* **`| user-device-release { before-r99 failure-code`** *`code`* **`| r99-or-later failure-code`** *`code`* **`} ]`**

`remove`

This keyword causes the configuration to be deleted from the call control profile configuration.

`failure-code` *`cause_code`*

`cause_code:` Enter an integer from 2 to 111; default code is 13 (roaming not allowed in this location area [LA]).
Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 - MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated

- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

---

user-device-release { before-r99 | r99-or-later } failure-code *code*

Enables the SGSN to assign a reject cause code based on the detected 3GPP release version of the MS equipment.
One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111. Refer to the list above.

- **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111. Refer to the list above.

Usage

Use this command to define GMM reject cause codes when rejection is due to regional subscription information failure.

Example

The following command sets a location area rejection message, code 12 for regional restriction rejections:

```
regional-subscription-restriction failure-code 12
```

reuse-authentication-triplets

Creates a configuration entry to enable or disable the reuse of authentication triplets in the event of a failure.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | remove } reuse-authentication-triplets no-limit
```

no

Disables this configuration entry and disables reuse of authentication triplets.

remove

This keyword causes the reuse configuration to be deleted from the call control profile configuration. This is the default behavior. Triplets are reused.

no-limit

This keyword enables reuse triplets as needed.

Usage

Use this command to enable reuse of authentication triplets.

Example

```
reuse-authentication-triplets no limit
```

rfsp-override

Configures RAT frequency selection priority override parameters for this call control profile.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

rfsp-override { default | ue-val *value* **new-val** *value* **+ }**

remove rfsp-override { default | ue-val *value*

remove

Deletes the rfsp-override configuration from the call control profile.

default

Restores the default value assigned.

ue-val *value*

Assign the UE value for the RAT frequency selection priority.
value: Enter an integer from 1 to 256.

new-val *value*

Assign a new value for the RAT frequency selection priority as an integer from 1 to 256.

Usage

Use this command to configure the RAT frequency selection priority override parameter. Multiple UE value/new value combinations can be configured.

Example

Reset the default value for the RAT frequency selection priority override function:

```
rfsp-override default
```

s1-reset

Configures the behavior of user equipment (UE) on S1-reset.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

```
s1-reset { detach-ue | idle-mode-entry }

default s1-reset
```

default

Reset the profile configuration to the system default of **idle-mode-entry**.

detach-ue

Upon S1-reset the MME will detach the UE.

idle-mode-entry

Upon S1-reset the MME will move the UE to idle-mode. This is the default setting for this command.

Usage

Use this command to set the MME's reactions to an S1-reset.

Example

Configure the MME to put the UE into idle-mode upon receipt of S1-reset:

```
s1-reset idle-mode-entry
```

sctp-down

Configures the behavior towards UE (user equipment) when Stream Control Transmission Protocol (SCTP) goes down.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

```
sctp-down { detach-ue | idle-mode-entry }

default sctp-down
```

default

Reset the profile configuration to the system default when SCTP layer goes down. The default for this command is **idle-mode-entry**.

detach-ue

When SCTP goes down, the MME will detach the UE.

idle-mode-entry

When the SCTP goes down, the MME will move the UE to idle-mode. This is the default for this command.

Usage

Use this command to set the MME's reactions when the SCTP goes down.

Example

Configure the MME to put the UE into idle-mode when the SCTP layer goes down:

```
sctp-down idle-mode-entry
```

sgsn-address

Defines the IP addresses for peer SGSNs in a static SGSN address table. These configured addresses can be used rather than using DNS.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
sgsn-address rac rac-id lac lac_id [ nri nri ] prefer { fallback-for-dns | local }
address { ipv4 ip_address | ipv6 ip_addess }

no sgsn-address { ipv4 ip_address | ipv6  ip_addess } rac  rac_id lac lac_id [ nri nri
```

no

Disables the peer-SGSN address configuration for the designated IP address.

rac *rac_id*

Identifies the foreign routing area code (RAC) of the peer-SGSN address to be configured in the static peer-SGSN address table. *rac_id* must be an integer from 1 to 255.

lac *lac_id*

Identifies the foreign location area code (LAC) ID of the peer-SGSN address to be configured in the static peer-SGSN address table. *lac_id* must be an integer from 1 to 65535.

nri *nri*

Identifies the network resource identifier stored in the P-TMSI (bit 17 to bit 23). *nri* must be an integer from 0 to 63.

Important: Typically, use of this keyword is optional. However, it must be included in the command when Flex (SGSN-Pooling) is implemented.

prefer

Indicates the preferred source of the address to be used.

- **fallback-for-dns** -

  Important: The **fallback-for-dns** option is under development for future use and is not supported in this release.

- **local** - instructs the system to use the local IP address configured with this command.

address *ip_address*

- **ipv4** - specifies a valid address in IPv4 dotted-decimal notation.

- **ipv6 -**

  Important: The **ipv6** option is under development for future use and is not supported in this release.

Usage

Use this command to save time by avoiding DNS. This command enables a local mapping by setting the peer-SGSN IP address to be used for inter-SGSN Attach and inter-SGSN-RAU. When configured, if the SGSN receives a RAU or an Attach Request with a P-TMSI and an old-RAI that is not local, the SGSN consults this table and uses the configured IP address instead of resolving via DNS. If this table is not configured, then IP address resolution is done using DNS.

The MCC and MNC of the RAI are taken from the IMSI range configured in the operator policy and the LAC and RAC are configured here in the call control profile configuration mode.

The **sgsn-address** command differs from other Call Control Profile configuration mode commands in the following ways:

- Within the SGSN's call logic, all other configuration elements defined with the other commands in this mode are used *after* the IMSI is learnt. The configuration defined with this command is part of the decision logic *prior* to the IMSI being known.
- With the peer-SGSN address configured using this **sgsn-address** command, the peer-SGSN-RAI's MCC/MNC is used as a 5 or 6-digit IMSI and the operator policy and call control profile selection are completed.

Important: Typically, use of this command is optional. However, it must be included in the configuration when Flex (SGSN-Pooling) is implemented if (1) the SGSN functions as a default SGSN, then configure the local-NRI of other SGSN with this command; or if (2) another SGSN is offloading, then configure the NB-RAI/null-NRI of the peer-SGSN with this command.

Example

Create a local peer-SGSN address mapping of an RAI with RAC of *123* and LAC of *4444* and an *IPv4* address of *123.11.313.11* for the peer-SGSN:

```
sgsn-address rac 123 lac 4444 local address ipv4 123.11.313.11
```

sgsn-core-nw-interface

This command is under development and not yet supported for configuration.

Product

SGSN

Privilege

Security Administrator, Administrator

sgsn-number

Defines the SGSN's E.164 number to be used for interactions via the Mobile Application Part (MAP) protocol. E.164 is an ITU-T recommendation that defines the international public telecommunication numbering plan used in public switched telephone networks (PSTN) and some other data networks.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sgsn-number *E164_number*

no sgsn-number

no

Disables the use of this configuration definition.

E164_number

Specifies a string of 1 to 16 digits that serve as the SGSN's E.164 identification.

Usage

This command configures the current SGSN E164 contact number.
The SGSN number configured for a call control profile is related to the SGSN number configured in the SGSN service configuration and/or in the GPRS service configuration. If the SGSN number is not configured as part of the call control profile configuration, then the SGSN number defined as part of the SGSN service or GPRS service configuration is used.
When the 3G SGSN supports multiple PLMNs configured through different IuPS services or when network sharing is implemented, then it may be required to use different SGSN numbers for each PLMN. In such cases, configure the per-PLMN SGSN number in a call control profile. SGSN number definition for a call control profile allows emulation of a different SGSN to each HLR per PLMN. SGSN number definitions in the call control profile also enable the SGSN to use a different SGSN number per operator when network sharing is implemented.

Example

Map the E.164 number *198765432123456* for the SGSN to this call control profile configuration:

```
sgsn-number 198765432123456
```

sgtp-service

Identifies the SGTP service configuration to be used according to this call control profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sgtp-service context *ctxt_name* **service** *sgtp_service_name*

no sgtp-service context

context *ctxt_name*

Specifies the SGTP context as an alphanumeric string of 1 through 64 characters.

service *sgtp_service_name*

Specifies the SGTP service name as an alphanumeric string of 1 through 64 characters.

no

Disables use of SGTP service.

Usage

Use this command to configure enabling or disabling of SGTP service for this call control profile.

Example

```
sgtp-service context sgtp1 service sgtp-srvc1
```

sms-mo

Configures how mobile-originated (MO) short message service (SMS) messages are handled.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ remove ] sms-mo { { access-type { gprs | umts } { all-location-areas | location-area-
list } | allow access-type { gprs | umts } | restrict access-type { gprs | umts } }
```

remove

Deletes the specified configuration.

access-type *type*

Access by SMS will be limited to SMS coming from this network type:

- **gprs**
- **umts**

allow

Allow either GPRS or UMTS type access for SMS.

restrict

Restrict either GPRS or UMTS type access for SMS.

location-area-list instance *instance*

instance must be an integer between 1 and 5. The value must identify an already defined location area code (LAC) list created with the **location-area-list** command.

failure-code *code*

code: Must be an integer from 2 to 111.

Usage

Configure filtering for SMS-MO messaging.

Example

```
sms-mo access-type gprs all-location-areas failure-code 100
```

sms-mt

This command configures how mobile-terminated (MT) short message service (SMS) messages are handled.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ remove ] sms-mt { { access-type { gprs | umts } { all-location-areas | location-area-
list } | allow access-type { gprs | umts } | restrict access-type { gprs | umts } }
```

remove

Deletes the specified configuration.

access-type *type*

Access by SMS will be limited to SMS coming from this network type:

- **gprs**
- **umts**

allow

Allow either GPRS or UMTS type access for SMS.

restrict

Restrict either GPRS or UMTS type access for SMS.

location-area-list instance *instance*

instance must be an integer between 1 and 5. The value must identify an already defined LAC list created with the **location-area-list** command.

failure-code *code*

code: Must be an integer from 2 to 111.

Usage

Configure filtering for SMS-MT messaging.

Example

```
sms-mt access-type gprs all-location-areas failure-code 100
```

srns-inter

Defines handling parameters for Inter-SRNS (Serving Radio Network Subsystem) relocation.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

srns-inter (all failure-code | allow location-area-list instance *instance* **| location-area-list instance** *instance* **failure-code** *code* **| restrict location-area-list instance** *instance* **}**

no srns-inter { allowlocation-area-list instance *instance* **| restrictlocation-area-list instance** *instance* **}**

default srns-inter { all | location-area-list-instance *instance* **}**

no

Deletes the inter-SRNS relocation configuration.

default

Resets the configuration to default values.

all failure-code *code*

Define the failure code that will apply to all inter-SRNS relocations.
code: Must be an integer from 2 to 111.

allow location-area-list instance *instance*

Identify the location area list Id (LAC Id) that will allow services in the defined location area.

location-area-list instance *instance*

instance: Must be an integer between 1 and 5 that identifies the previously defined location area list created with the **location-area-list** command.

restrict location-area-list instance *instance*

Identify the location area list Id (LAC Id) that indicates the location areas where services will be restricted.

Usage

This command defines the operational parameters for inter-SRNS relocation.

Example

The following command allows services in areas listed in LAC list #3:

```
srns-inter allow location-area-list instance 3
```

srns-intra

Defines handling parameters for intra-SRNS (Serving Radio Network Subsystem) relocation.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

srns-intra (all failure-code | allow location-area-list instance *instance* **| location-area-list instance** *instance* **failure-code** *code* **| restrict location-area-list instance** *instance* **}**

no srns-intra { allow location-area-list instance *instance* **| restrictlocation-area-list instance** *instance* **}**

default srns-intra { all | location-area-list-instance *instance* **}**

no

Deletes the intra-SRNS relocation configuration.

default

Resets the configuration to default values.

all failure-code *code*

Define the failure code that will apply to all intra-SRNS relocations.
code: Must be an integer from 2 to 111.

allow location-area-list instance *instance*

Identify the location area list Id (LAC Id) that will allow services in the defined location area.

location-area-list instance *instance*

instance: Must be an integer between 1 and 5 that identifies the previously defined location area list created with the **location-area-list** command.

restrict location-area-list instance *instance*

Identify the location area list Id (LAC Id) of the target RNC to determine the location areas where services will be restricted.

Usage

This command defines the operational parameters for intra-SRNS relocation.

Example

The following command restricts service in areas listed in the LAC list 1:

```
srns-intra restrict location-area-list instance 1
```

subscriber-control-inactivity

Configures \the subscriber-control inactivity timer. The system detects inactivity when no PDP context is activated and starts the timer.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

subscriber-control-inactivity timeout minutes *time* **detach { immediate | next-connection | reattach-time-period }**

{ no | default } subscriber-control-inactivity

---

no

Deletes the timer configuration.

---

default

Resets the timer configuration to the default value of 7 days (10080 minutes).

---

timeout minutes *time***[detach]**

Sets the number of minutes the SGSN monitors the connection after inactivity has been detected. When the timer expires, the subscribe will be detached.
time: Enter an integer from 1 to 20160 (two weeks).

---

detach [immediate | next-connection | reattach-time-period]

Instructs the SGSN to detach and can be configured to specify when the detach will occur after inactivity is detected. To fine-tune the detach instruction, include one of the following with the command:

- **immediate** - Instructs the SGSN to detach immediately after inactivity is detected. May combine with **reattach-time-period**.
- **next-connection** - instructs the SGSN to detach after the next Iu connection after inactivity is detected.

  Important: Supported for 3G SGSNs only.

- **reattach-time-period** *period***[action]** - Specify the number of seconds the SGSN will monitor a new re-attach after the previous detach was due to inactivity. Also, you can define the action to be taken regarding new attaches.

  period: Enter an integer from 60 to 3600.

  action - Select an action:

  - **deny**
  - **permit-and-stop-monitoring**

Usage

Use this command to configure the timeout timer. After this timer times out the subscriber is detached from the SGSN.

Example

The following command instructs the SGSN to monitor the connection for up to *360* minutes after inactivity is detected, or detach immediately after inactivity is detected:

```
subscriber-control-inactivity timeout minutes 360 detach immediate
```

super-charger

Enables or disables the SGSN to work with a super-charged network.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ remove ] super-charger
```

remove

Disables the super-charger functionality.

Usage

By enabling the super charger functionality for 2G or 3G connections controlled by an operator policy, the SGSN changes the hand-off and location update procedures to reduce signalling traffic management.

Example

The following command enables the super charger feature:

```
super-charger
```

tau

Configure parameters for the tracking area update (TAU) procedure.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

```
tau { imei-query-type { imei | imei-sv | none } [ verify-equipment-identity [ allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency ] ] | inter-rat security-ctxt { allow-mapped | native } }

remove tau { imei-query-type | inter-rat security-ctxt }
```

remove

Deletes this TAU configuration from the call control profile.

imei-query-type { imei | imei-sv | none }

This keyword set is specific to the MME.
Sets the IMEI query-type if an IMEI (International Mobile Equipment Identity) is not already present.

- **imei**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).
- **none**: Specifies that the MME does not need to query for IMEI or IMEI-SV.

verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]

Specifies that the identification (IMEI or IMEI-SV) of the UE is to be performed by the Equipment Identity Register (EIR) over the S13 interface.

- **allow-on-eca-timeout**: Configures the MME to allow equipment that has timed-out on ECA during the attach procedure.
- **deny-greylisted**: Configures the MME to deny grey-listed equipment during the attach procedure.
- **deny-unknown**: Configures the MME to deny unknown equipment during the attach procedure.
- **verify-emergency**: Configures the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases. This keyword is only supported in release 12.2 and higher.

inter-rat security-ctxt { allow-mapped | native }

Configure inter-RAT parameters for TAU. This keyword provides the operator with the option of continuing with the mapped context or creating a new native context after an inter-RAT handover.

- **allow-mapped**: Configures inter-RAT security-context type as mapped. Mapped security context is allowed after inter-RAT handover. This is the default value.

- **native**: Configures inter-RAT security-context type as native only. Inter-RAT handover will always result in a native security context.

Usage

Use this command to define tracking area update procedures such as inter-RAT security context and IMEI query-type.

Example

The following command sets the IMEI query type to IMEI-SV:

```
tau imei-query-type imei-sv verify-equipment- identity
```

treat-as-hplmn

Enables or disables the MME or SGSN to treat an IMSI series as coming from the home PLMN.

Product

MME, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ remove ] treat-as-hplmn
```

remove

Deletes this configuration from the profile. This would disable this function and is the default.

Usage

Use this command to enable or disable the MME/SGSN to treat an IMSI series as coming from the home PLMN.

Example

The following command disables previously configured feature:

```
remove treat-as-hplmn
```

zone-code

Configures a zone code listing of one or more location area code (LACs) included in the zone.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

zone-code *zc_id* **location-area-code** *lac*

no zone-code *zc_id* **[location-area-code** *lac* **]**

no

Removes either a specific LAC from the zone code list. If the **location-area-code** parameter is not included in the command, then the entire zone code list definition is removed from configuration.

zc_id

Identifies an instance of a zone code list as an integer from 1 to 65535.
An unlimited number of zone code lists can be configured per call control profile as the zone code lists are allocated dynamically. A maximum of 10 zone code lists can be configured per Call Control Profile.

location-area-code *lac*

Prompts for the location area-code(s), where the subscribers can roam, that are part of the zone. *lac* is an integer from 1 to 65535.
Repeat the command with this parameter to include up to 100 LACs in the zone code list.

Usage

Important: While there is no limit to the number of zone codes that can be created, only 10 LACs per zone code can be defined.

Use this command to define zone code restrictions. Regional subscription data at the home location register (HLR) is used to determine the regional subscription area in which the subscriber is allowed to roam. The regional subscription data consists of a list of zone codes. A zone code is comprised of one or more location areas (identified by a LAC) into which the subscriber is allowed to roam. Regional subscription data, if present in the insert subscriber data (ISD) request from the HLR, defines the subscriber's subscription area for the addressed SGSN. It contains the complete list (up to 10 zone codes) that apply to a subscriber in the currently visited PLMN.
During the GPRS Location Update procedure, the zone code list is received in the ISD request from the HLR. The zone code list from the HLR is validated against the configured values in the operator policy. If matched, then the ISD is allowed to proceed. If not matched, then the ISD response is that the Network Node Area is Restricted and the GPRS Location Update procedure fails. If no zone codes are included in the ISD (whether or not the zone codes are defined in the SGSN configuration), then checking is not done.

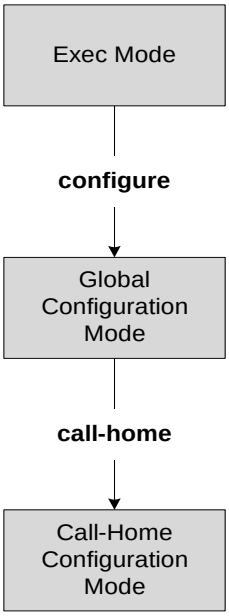
Example

The following command defines multiple LACs for zone code 1:

```
zone-code 1 lac 413 212 113
```

Chapter 44
Call-Home Configuration Mode

The Call-Home Configuration Mode sets parameters for the Smart Call Home feature. Smart Call Home is a contracted service that sends real-time alerts, remediation, and personalized web-based reports to the Cisco Technical Assistance Center (TAC) and other configured receivers.



activate

Activates the Cisco Smart Call Home service.

Product

All

Privilege

Security Administrator, Administrator

Syntax

activate

default activate

no activate

default

Configures the call-home service back to default settings.

no

Disables the call-home services.

activate

Enables the call-home services.

Usage

Use this command to enable the call-home services.

Example

The following command disables the call-home service:

```
no activate
```

alert-group

Enables or disables the Smart Call Home alert-group.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[default | no] alert-group { all | configuration | crashinfo | diagnostic | environment | inventory | syslog }

default

Configures the alert-group back to default settings. The default is enabled.

no

Disables the alert-groups.

alert-group all

Enables an alert group for all categories.

alert-group configuration

Enables an alert group related to configuration.

alert-group crashinfo

Enables an alert group related to crashes.

alert-group diagnostics

Enables an alert group related to diagnostics.

alert-group environment

Enables an alert group related to environment. These typically include events related to power, fan, and temperature alarms.

alert-group inventory

Enables an alert group related to inventory. This is a non-critical event that could include notifications when cards are inserted or removed, or when the system is cold-booted.

alert-group syslog

Enables an alert group related to syslog. This includes events generated by the syslog PORT facility.

Usage

An alert group is a predefined subset of Smart Call Home alerts that are supported on this device. Alert groups allow you to select the set of Smart Call Home alerts that you want to send to a predefined or custom destination profile.

Example

The following command enables alerts for all of the preconfigured Smart Call Home alerts:

```
alert-group all
```

contact-email-addr

Sets the e-mail address of the person identified as the prime contact for this system.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] contact-email-addr *email_addr*

no

Removes the contact e-mail address.

contact-email-addr *email_addr*

Specifies the information for prime contact as an alphanumeric string in the format *local-part@domain*, where domain can be made up of a number of labels, each separated by a period and between 1 and 63 characters in length. The local-part can be 1-64 characters. The domain-label can be 1-63 characters. The domain can be 1 through 135 characters. The entire alphanumeric string can be a no larger than 200 characters.

Usage

Use this command to set up the e-mail address for the person identified as the contact person for this device.

Important: You can enter any valid e-mail address. You cannot use spaces.

Example

The following command specifies e-mail address for the entity *notity.TAC@NOCservices.net*:

```
contact-email-addr notity.TAC@NOCservices.net
```

contract-id

Configures the system's contract-identifier for Cisco AutoNotify.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[default | no] contract-id *contractID*

default

Configures the call-home contract-id back to default settings.

no

Removes the call-home contract-id.

contract-id *contractID*

Specifies the call-home contract-id as an alphanumeric string of 1 through 64 characters that is case sensitive. If you include spaces in this string, you must enclose it in double quotation marks.

Usage

Use this command to enter this system's AutoNotify contract ID.

Example

The following command specifies the contract-id as *Contract1234_ID*:

```
contract-id Contract1234_ID
```

customer-id

Configures the system's customer-identifier for Cisco AutoNotify.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[default | no] customer-id *customerID*

default

Configures the call-home customer-id back to default settings.

no

Removes the call-home customer-id.

customer-id *customerID*

Specifies the call-home customer-id as an alphanumeric string of 1 through 64 characters that is case sensitive. If you include spaces in the string, you must enclose it in double quotation marks.

Usage

Use this command to set up the system's customer ID for Cisco's AutoNotify.

Example

The following command specifies the customer-id as *CustID_1234*:

```
customer-id CustID_1234
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

mail-server

Configures the Smart Call Home mail-server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] mail-server *server_name* **priority** *priority_num*

no

Removes the call-home mail-server.

mail-server *server_name*

Identifies the mail server as an alphanumeric string of 1 through 64 characters. The server ID can take the form of a host name (DNS) or an IPv4 address in dotted-decimal notation.

priority

Sets the mail server priority order as an integer from 1 (highest) to 100 (lowest).

Usage

Use this command to set up the mail server for Smart Call Home. This configuration is mandatory when the user profile is configured to only send out e-mail messages.

Example

The following command specifies the mail-server as *10.2.3.4* with a priority of *1*:

```
mail-server 10.2.3.4 priority 1
```

phone-number

Enables or disables the phone-number for the Smart Call Home contact person.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no | default] phone-number *phone-number-string*

default

Configures the phone number back to default settings. The default is enabled.

no

Removes the call-home phone number.

phone-number *phone-number-string*

Specifies the phone number for the contact person for this system as an alphanumeric string that can only contain: + (plus sign), - (dash) and numbers. The total length of the string is 12 to 16 characters. If you include spaces, you must enclose the string in double quotation marks.

Usage

Use this command to set up the phone number for Smart Call Home contact.

Example

The following command specifies the phone number as *+866-111-2234*:

```
phone-number 866-111-2234
```

profile

Creates the Smart Call Home profile.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] profile *profile_name*

no

Removes the call-home profile.

profile *profile_name*

Creates or modifies the profile name for this system as an alphanumeric string of 1 through 31 characters.

Usage

Use this command to create a new profile or modify an existing profile. This command moves you to the Call-Home Profile Configuration mode.

Example

The following command creates a profile named *Profile_1*:

```
profile Profile_1
```

rate-limit

Enables or disables the message rate-limit for Smart Call Home features.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no | default] rate-limit *message_count*

default

Sets the rate limit back to the default of 20 messages per minute.

no

Removes the call-home rate-limit.

rate-limit *message_count*

Sets the rate limit in messages per minute. *message_count* is an integer from 1 to 60. Default: 20

Usage

Use this command to configure the call-home message rate limit per minute. The default is 20 messages per minute.

Example

The following command sets the call-home rate limit to *10*:

```
rate-limit 10
```

sender

Specifies the Smart Call Home e-mail settings for the “from” address and “reply-to” address.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no | default] sender { from *email_address* **| to** *email_address* **}**

default

Sets the sender back to the default.

from *email_address*

Sets the sender’s reply from address.

no

Removes the call-home sender.

to *email_address*

Sets the sender’s reply-to address.

email_address

This is an alphanumeric string in the format *local-part@domain*, where domain can be made up of a number of labels, each separated by a period and between 1 and 63 characters in length. The local-part can be 1-64 characters. The domain-label can be 1-63 characters. The domain can be 1 through 135 characters. The entire alphanumeric string can be a no larger than 200 characters.

Usage

Use this command to specify the e-mail settings for the sender. This command sets the “to” and “from” fields in the e-mail.

Example

The following command sets the from address to *notity.TAC@NOCservices.net* and the reply-to address to *support@cisco.com*:

```
semder from notity.TAC@NOCservices.net to support@cisco.com
```

site-id

Specifies the Smart Call Home site identifier for this system.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[default | no] site-id *siteID*

default

Sets the site-id back to the default.

no

Removes the call-home site-id.

site-id *siteID*

Specifies the site ID as an alphanumeric string of 1 through 200 characters. If you include spaces, then you must enclose your entry in quotes.

Usage

Use this command to specify the Smart Call Home site identifier for this system.

Example

The following command sets the site-id to *NOC_Services_site_1011*:

```
site id NOC_Services_site_1011
```

street-address

Specifies the Smart Call Home street address for the system.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[default | no] street-address *streetADR*

default

Sets the street-address back to the default.

no

Removes the call-home street-address.

street-address *streetADR*

Specifies e Smart Call Home street-address as an alphanumeric string of 1 through 200 characters. You can include the street address, City, State, and ZIP Code. If you include spaces, then you must enclose the string in double quotation marks.

Usage

Use this command to set up the street address for the system.

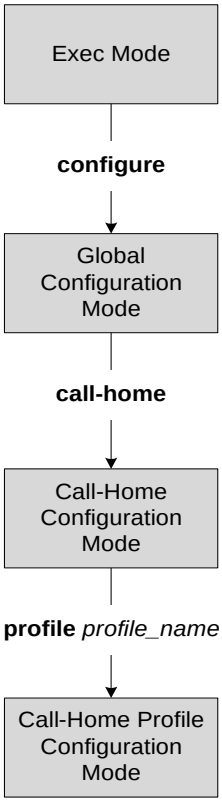
Example

The following command sets the street address to *123 Main St., Chicago, IL 60000*:

```
street-address "123 Main St., Chicago, IL 60000"
```

Chapter 45
Call-Home Profile Configuration Mode

The Call-Home Profile Configuration Mode is used to create groups of users that will receive alerts when events occur. The Smart Call Home service sends real-time alerts, remediation, and personalized web-based reports to the Cisco Technical Assistance Center (TAC) and other configured receivers.



active

Activates this Smart Call Home profile.

Product

All

Privilege

Security Administrator, Administrator

Syntax

active

default active

no active

default

Configures the call-home profile back to default settings. By default, the profile is enabled.

no

Deletes the call-home profile.

activate

Activates this Smart Call Home profile.

Usage

Use this command to activate or deactivate this call-home profile. By default, the profile is enabled.

Example

The following command disables the call-home profile:

```
no active
```

destination

Configures the message destinations for this Smart Call Home profile.

Product

All

Privilege

Security Administrator, Administrator

Syntax

destination [address [email *email_address* **| http** *http_url* **] | message-size-limit** *size* **| preferred-msg-format [long-text | short-text | xml] | transport-method [email** *email_address* **| http** *http_url***]]**

default destination [message-size-limit | preferred-msg-format | transport-method]

no destination [address [email *email_address* **| http** *http_url* **] | message-size-limit** *size* **| preferred-msg-format [long-text |short-text | xml] | transport-method [email** *email_address* **| http** *http_url* **]]**

---

address [email *email_address* **| http** *http_url* **]**

Configures an destination e-mail address or HTTP URL where short-text/long-text call-home message and XML-based call-home messages will be sent.

- **email**: Use this option to add an e-mail address to this profile. *email_addr* is an alphanumeric string of the form *local-part@domain* where domain can be made up of a number of labels, each separated by a period and between 1 and 63 characters in length. The local-part can be 1-64 characters. The domain-label can be 1-63 characters. The domain can be 1-135 characters. The entire alphanumeric string can be a no larger than 200 characters.
- **http**: Use this option to add an HTTP URL to this profile. *http_url* is an alphanumeric string of 1 through 200 characters.

---

default

Configures the call-home profile back to default settings. By default, the profile is enabled.

---

message-size-limit *size*

Specifies the message size (in bytes) for this profile as an integer from 50 to 3145728. The default is 3145728.

---

no

Deletes the call-home profile.

---

preferred-msg-format [long-text | short-text | xml]

Specifies the message format for the profile. The default is xml.

- **long-text**: Use this option to set long-text messages as the preferred message format. The long message format has all the details related to the event, including information related to chassis, card, and outputs of show commands for the alert group.

- **short-text**: Use this option to set short-text messages as the preferred message format. The short message has information on the severity of event, a short description of the event, the event time, and the device ID.
- **xml**: Use this option to set XML as the preferred message format. (Default)

transport-method [email *email_address* **| http** *http_url***]]**

Specifies the transport-method for the messages. The default is e-mail. For the user profile, both e-mail and http can be enabled. If all are options are disabled, e-mail will be set for the profile.
For the Cisco TAC profile, only one transport method can be enabled. If the user enables a second transport method, the first one will be automatically disabled.

- **email**: Enables an e-mail address for this profile. This is the default.
- **http**: Enables an HTTP URL for this profile.

Usage

Use this command to activate the current call-home profile. By default, the profile is enabled.

Example

The following command disables the call-home profile:

```
no destination
```

The following command sets the preferred message format for the profile to the call-home profile to short text:

```
destination preferred-msg-format short-text
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

subscribe-to-alert-group

Subscribes this profile to the alert group for the call-home profile.

Product

All

Privilege

Security Administrator, Administrator

Syntax

subscribe-to-alert-group [all {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] } | configuration { periodic [daily | monthly | weekly] } | crashinfo | diagnostic { severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] } | environment { severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] } | inventory { periodic [daily | monthly | weekly] } | syslog {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] }]

default subscribe-to-alert-group

no subscribe-to-alert-group [all {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] } | configuration { periodic [daily | monthly | weekly] } | crashinfo | diagnostic {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] } | environment {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] } | inventory { periodic [daily | monthly | weekly] } | syslog {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] [pattern *pattern_to_match*] }]

---

all {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] }

Enables call-home messages based for all group-types and severity for the profile. The following severities are supported:

- **catastrophic**– Level 1: catastrophic event, matches platform logging level critical.
- **disaster** – Level 2: disaster event, matches platform logging level critical.
- **fatal** – Level 3: fatal event, matches platform logging level critical.
- **critical** – Level 4: critical event, matches platform logging level critical.
- **major** – Level 5: major event, matches platform logging level error.
- **minor** – Level 6: minor event, matches platform logging level warning.
- **warning** – Level 7: warning event, matches platform logging level warning.
- **notification** – Level 8: notification event, matches platform logging level unusual.
- **normal** – Level 9: normal event, matches platform logging level info.

configuration { periodic [daily | monthly | weekly] }

Enables call-home messages based for configuration alert groups. The messages are sent at periodic intervals such as:

- **daily**: Sends a daily call-home message.
- **monthly**: Sends a monthly call-home message.
- **weekly**: Sends a weekly call-home message.

crashinfo

Configures the call-home profile back to default settings. By default, the profile is enabled.

default

Restores the parameter back to the default value.

diagnostic { severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] }

Enables call-home messages based for diagnostic group-types and severity for the profile. The following severities are supported:

- **catastrophic**– Level 1: catastrophic event, matches platform logging level critical.
- **disaster** – Level 2: disaster event, matches platform logging level critical.
- **fatal** – Level 3: fatal event, matches platform logging level critical.
- **critical** – Level 4: critical event, matches platform logging level critical.
- **major** – Level 5: major event, matches platform logging level error.
- **minor** – Level 6: minor event, matches platform logging level warning.
- **warning** – Level 7: warning event, matches platform logging level warning.
- **notification** – Level 8: notification event, matches platform logging level unusual.
- **normal** – Level 9: normal event, matches platform logging level info.

environment {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] }

Enables call-home messages based for environment group-types and severity for the profile. The following severities are supported:

- **catastrophic**– Level 1: catastrophic event, matches platform logging level critical.
- **disaster** – Level 2: disaster event, matches platform logging level critical.
- **fatal** – Level 3: fatal event, matches platform logging level critical.
- **critical** – Level 4: critical event, matches platform logging level critical.
- **major** – Level 5: major event, matches platform logging level error.
- **minor** – Level 6: minor event, matches platform logging level warning.
- **warning** – Level 7: warning event, matches platform logging level warning.
- **notification** – Level 8: notification event, matches platform logging level unusual.
- **normal** – Level 9: normal event, matches platform logging level info.

inventory { periodic [daily | monthly | weekly] }

Enables call-home messages based for inventory alert groups. The messages are sent at periodic intervals such as:

- **daily**: Sends a daily call-home message.
- **monthly**: Sends a monthly call-home message.
- **weekly**: Sends a weekly call-home message.

no

Deletes the alert groups.

syslog { severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] [pattern *pattern_to_match*] }]

Enables and disables call-home messages based on severity and syslog string pattern match for the profile. The following severities are supported:

- **catastrophic**– Level 1: catastrophic event, matches platform logging level critical.
- **disaster** – Level 2: disaster event, matches platform logging level critical.
- **fatal** – Level 3: fatal event, matches platform logging level critical.
- **critical** – Level 4: critical event, matches platform logging level critical.
- **major** – Level 5: major event, matches platform logging level error.
- **minor** – Level 6: minor event, matches platform logging level warning.
- **warning** – Level 7: warning event, matches platform logging level warning.
- **notification** – Level 8: notification event, matches platform logging level unusual.
- **normal** – Level 9: normal event, matches platform logging level info.

pattern_to_match is an alphanumeric string of 1 through 80 characters.

Usage

Use this command to enable or disable the call-home messages based on specified alert-groups and severities for the profile.

Example

The following command sets an alert group for the profile to send a daily inventory message:

```
subscribe-to-alert-group inventory periodic daily
```

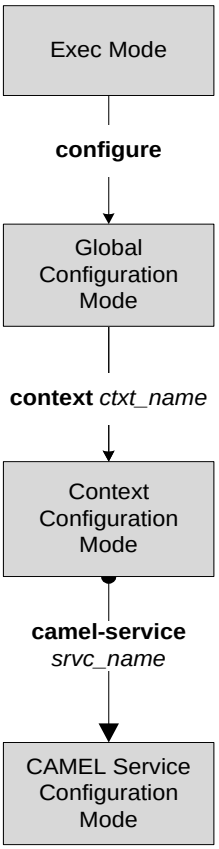
Chapter 46
CAMEL Service Configuration Mode Commands

The CAMEL Service configuration mode provides a set of commands to define the parameters for the Customised Applications for Mobile networks Enhanced Logic (CAMEL) service functionality and the CAMEL interface - the Ge interface.

CAMEL service enables operators of 2.5G/3G networks to provide operator-specific services (such as prepaid GPRS service and prepaid SMS service) to subscribers, even when the subscribers are roaming outside their home public land mobile network (HPLMN).

When this mode is accessed, the command prompt should resemble:

```
[context_name]asr5000(config-camel-service)#
```



associate-sccp-network

Configure an association between this CAMEL service and a specified SCCP network.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

associate-sccp-network *sccp_network_id*

no associate-sccp-network

no

Removes the association with the CAMEL service configuration.

sccp_network_id

Identifies an already defined SCCP network.
sccp_network_id : Enter an integer from 1 to 12.

Usage

The SCCP network must be configured prior to use this command.
CAMEL service will not function unless an SCCP network is associated.

Example

Associate this CAMEL service with SCCP network configuration ID 2:

```
associate-sccp-network 2
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Return to the Exec mode.

exit

Exits the current configuration mode and returns to the context configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Move to the previous configuration mode.

tcap destination-address

Configure the gsmSCF address to be used to open TC dialogues.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
tcap destination-address { configured-address | received-address }

default tcap destination-address
```

configured-address

Default.
Instructs the SGSN to use the SCF address from the GPRS-CSI.

received-address

Instructs the SGSN to overwrite the gsmSCF address with the memorised gsmSCF address that was in the first response message to the InitialDPGPRS and then to use that gsmSCF address.

Usage

This command enables the operator to determine which gsmSCF address is to be used to open new TC dialogues. In accordance with 3GPP 29.078, section 14.1.4.1.3, this command enables the SGSN to establish new TC dialogues within the context of a current GPRS dialogue, based on the operators choice:

- to use a 'received-address' where the gprsSSF learns the gsmSCF address used in the first response message to the InitialDPGPRS and uses it to open new TC dialogues, or
- to use a 'configured-address' where the gprsSSF uses the gsmSCF address from the GPRS-CSI to open new TC dialogues.

Example

Configure the SGSN to overwrite the SCF address and to use the gsmSCF address received in the response message:

```
tcap destination-address received-address
```

timeout

Configure a range of timers needed to support CAMEL service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

timeout { gprs-apply-charging-report-ack-timer *seconds* **| gprs-entity-release-ack-timer** *seconds* **| gprs-event-report-ack-timer** *seconds* **| gprs-tssf-timer** *seconds* **| sms-event-report-ack-timer** *seconds* **| sms-tssf-timer** *seconds* **| tc-guard-timer** *seconds* **}**

default timeout { gprs-apply-charging-report-ack-timer | gprs-entity-release-ack-timer | gprs-event-report-ack-timer | gprs-tssf-timer | sms-event-report-ack-timer | sms-tssf-timer | tc-guard-timer }

default

Resets the timers to default values.

gprs-apply-charging-report-ack-timer *seconds*

Configure the TCAP invoke timer to set the length of time the SGSN waits for an acknowledgement after sending an ApplyChargingReportGPRS to the SCF.
seconds : Enter an integer from 1 to 20. Default: 4

Important: This timer value should be less than the value configured for the `tc-guard-timer`.

gprs-entity-release-ack-timer *seconds*

Configure the TCAP invoke timer to set the length of time the SGSN waits for an acknowledgement from the SCF after sending Entity Release information.
seconds : Enter an integer from 1 to 20. Default: 4

gprs-event-report-ack-timer *seconds*

Configure the TCAP invoke timer to set the length of time the SGSN waits for an acknowledgement from the SCF after the SGSN sends an event report.
seconds : Enter an integer from 1 to 20. Default: 4

gprs-tssf-timer *seconds*

Configure the GPRS TSSF timer to set the length of time the SGSN waits for an instructions from the SCF. On expiry the SGSN handles the transaction through the default handling specified in the corresponding CSI.
seconds : Enter an integer from 1 to 10. Default: 5

sms-event-report-ack-timer *seconds*

Configure the TCAP invoke timer to set the length of time the SGSN waits for an acknowledgement from the SCF after the SGSN sends an event report for SMS.

seconds : Enter an integer from 1 to 20. Default: 4

sms-tssf-timer *seconds*

Configure the SMS TSSF timer to set the length of time the SGSN waits for an instructions from the SCF. On expiry the SGSN handles the transaction through the default handling specified in the corresponding CSI.
seconds : Enter an integer from 1 to 10. Default: 5

tc-guard-timer *seconds*

Configure the guard tier to start when the SGSN sends ApplyChargingReportGPRS to the SCF. On expiry the SGSN closes the TCAP dialogue if the GPRS Dialogue state is “monitoring”. Default handling complies with 3GPP 23.078.
seconds : Enter an integer from 1 to 10. Default: 5

Important: This timer value should be greater than the value configured for the `gprs-apply-charging-report-ack-timer`.

Usage

The SCCP network must be configured prior to use this command.
CAMEL service will not function unless an SCCP network is associated.
Repeat the command to configure multiple timers.

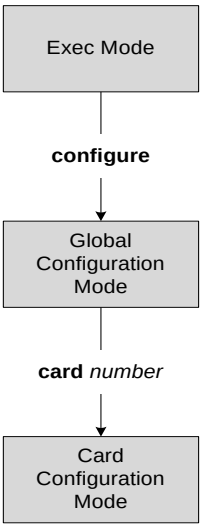
Example

Set the tc-guard timer for 4:

```
tc-guard-timer 4
```

Chapter 47
Card Configuration Mode Commands

Use the Card configuration mode to create and manage the physical cards in the chassis.



aps

Configures the parameters for the automatic protection switching (APS) feature for SONET CLC2 and OLC2 line cards or for multiplexed section (or switching) protection (MSP) type APS for SDH CLC2 and OLC2 line cards.

Important: This command should only be used **after** APS has been enabled with the **aps-mode** keyword of the redundancy command.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
aps [ 1+1 ] [ uni-directional ] [ non-revertive ] [ -noconfirm ]

no aps
```

1+1

Selects 1+1 line (linear) protection.Traffic is carried simultaneously by the working line and the protection line. GR-253 and ITU-T G.783 require the bridging to be done at the electrical level; therefore, the same payloads are transmitted over the working and protection lines.

uni-directional

Enables protection on one end of the connection.

non-revertive

Prevents the network from automatically reverting to the original working line/port when the the original working line/port is recovered/restored.

-noconfirm

Executes the command without additional prompting for command confirmation.

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

framing

Configures the type of framing to be used for the signaling generated on a specific line card.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
framing { ethernet | sdh [ ds1 | e1 ] [ ss-bits ] | sonet [ ds1 | e1 ] | unspecified } [
-noconfirm ]

default framing [ -noconfirm ]
```

default

Resets the framing generated by the card to the default for the particular card type.

ethernet

Configures the system to use Ethernet framing for this line card. This type of framing can only be used on an Ethernet card.
Default: Ethernet framing type is the default for an Ethernet line card.

Important: Using this keyword with an OLC/OLC2 or CLC/CLC2 takes the card offline.

sdh [ds1 | e1] [ss-bits]

Configures the system to use SDH signal framing for either an OLC/OLC2 or CLC/CLC2 line card in an SGSN.

Important: Using this keyword with an Ethernet line card takes the line card offline.

In releases 8.1 and higher, you can also set the type of signaling path for a CLC2.
ds1 - configures the card to support a DS1/T1.
e1 - configures the card to support an E1. This is the default for SDH.
ss-bits - enables/disables use of ss-bits (per ITU 1997 G.783 specification) for SDH configured line card.

sonet [ds1 | e1]

Configures the system to use SONET signal framing for either an OLC/OLC2 or CLC/CLC2 line card in an SGSN.
Default: SONET is the default framing type for an OLC/OLC2 or CLC/CLC2 line card.

Important: Using this keyword with an Ethernet line card takes the line card offline.

In releases 8.1 and higher, you can also set the type of signaling path for a CLC2.

ds1 - configures the card to support a DS1/T. This is the default for SONET.
e1 - configures the card to support an E1.

unspecified

Configures the system to use the default framing type for the particular line card resident in the identified slot.

-noconfirm

Instructs the system to execute the command without additional prompting for command confirmation.

Usage

Use the **framing** command to identify the type of signal framing to be used by the line card in the identified slot.
Note that each type of line card uses a different type of signal framing. If you configure the wrong framing type for a line card, the line card is taken offline.

Important: This command is not supported on all platforms.

Example

Use the following command to configure SDH signal framing on a CLC2. If you do not include the path-type, the default of **e1** is automatically included in the card's framing configuration:

```
framing sdh
```

header-type

Defines the size of the header frame for Frame Relay transmissions over a CLC or CLC2 channelized line card.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

header-type *header-size* [**-noconfirm**]

default header-type [-noconfirm]

default

Resets the configuration to the default header size of 2-bytes.

header-type *header-size*

Sets the size, number of bytes, for the header frame. *header-size* must be either 2-bytes or 4-bytes.

-noconfirm

Executes the command without additional prompting for command confirmation.

Usage

Use this command to set the size of the header frame for Frame Relay messages emanating from the line card. The size (2-bytes or 4-bytes) determines the amount of information that can be transmitted in that first information frame.

Important: Not supported on all platforms

Example

Set the header to the smallest size.

```
header-type 2-byte
```

initial-e1-framing

Configures the type of framing mode that will initially be available at the time the line card boots.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
initial-e1-framing [ crc4 | standard ]

default initial-e1-framing
```

default

Returns the configuration to CRC4 as the default type.

initial-e1-framing crc4

Accepts the default CRC4, in the configuration, as the initial at-boot framing mode.

initial-e1-framing standard

Accepts the **standard** mode as the initialization framing mode.

Usage

For a CLC-type line card, the default E1 framing mode is CRC4. When a card reboots, all E1s are initialized with CRC4 framing mode and then switch to the configured framing mode. With this keyword, you have the option to choose the initialization framing mode.

Important: Only supported on CLC/CLC2

Example

```
initial-e1-framing standard
```

link-aggregation

This command and its keywords are now obsolete. Configuring the link aggregation feature is now accomplished in two parts. The first part requires the configuration of master port options via the **link-aggregation** command in the Ethernet Port Configuration mode. The second part configures the switching options for network deployments with multiple network devices via the **link-aggregation switch to** command in the Exec mode. For additional information see the *System Administration Guide*.

mode

Sets the application processor card's current administrative state to active or standby.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
mode { active | standby } [ -noconfirm ]

default mode [ -noconfirm ]
```

default

Returns the mode to the default value appropriate to the card type.
The default administrative mode for line cards affects a single card and its mated line card. The default state for line cards in the top shelf is active. The default for line cards in the bottom shelf is standby.
The default administrative state for the SPIO in slot 24 is active and the SPIO in slot 25 is standby.
The default administrative mode for packet processing cards is standby.

Important: This command results in a migration of processes if the default mode for a card is different than the current state of the card.

mode active

Defines which card type is to be switched from standby to active state. If a card is present in the slot, the packet processing card is automatically selected depending upon the type of card. If no card is present in the slot, a packet processing card is assumed.

mode standby

Sets the packet processing card in the slot to standby mode.

Caution: Switching an active packet processing card to standby deletes all port configurations, including bindings, for the attached line cards.

-noconfirm

Executes the command without additional prompting for command confirmation.

Usage

Set the desired mode of mated cards. The card targeted for maintenance is placed in the standby state first. The setting of the mode determines which packet processing cards are to be active and which are to be the standby cards for redundancy. Use this command to configure the set of active and standby packet processing cards. The application processor card's standby priority is then used in conjunction with the set of standby packet processing cards to determine the order in which the standby cards are used for redundancy support.

Important: Not supported on all platforms

Important: This command results in a migration of processes if the mode specified for the card is different than the current state of the card.

Example

The following commands set the state of a card to active and standby, respectively.

```
mode active

mode standby
```

redundancy

Configures the type of redundancy for a line card or SPIO.

Product

PDSN, FA, HA, GGSN, SSGN

Privilege

Security Administrator, Administrator

Syntax

```
redundancy { aps-mode | card-mode |port-mode } [-noconfirm ]

default redundancy [ -noconfirm ]
```

default

Restores redundancy to **port-mode** type redundancy.

aps-mode

SGSN only.
Enables automatic protection switching (APS), if the card is either a CLC2 or an OLC2 line card with card framing set to SONET. (Refer to the framing command.)
Enables multiplexed section (or switching) protection (MSP) type APS, if the card is a CLC2 line card with card framing set to SDH. (Refer to the framing command.)

Important: Using this keyword with any card type other than a CLC2 or an OLC2 will take the card offline.

Related parameters: You should consider setting appropriate SDSF BER (signal degrade/signal failure bit error rate) threshold settings. Access the hopath-sdsf, lopath-sdsf, and toh-sdsf commands via the port channelized configuration mode -- for a CLC2 line card refer to the *Channelized Port Configuration Mode Commands* chapter and for an OLC2 line card refer to the *ATM Port Configuration Mode Commands* chapter.

card-mode

Specifies no port redundancy is used. This is used mostly for legacy products.

port-mode

Enables port redundancy on line cards or on SPIO cards.
This is the default setting used by the system.

Important: Port-type redundancy does not affect line card failover/redundancy operations.

pseudo-aps-mode

This command has been deprecated.

-noconfirm

Instructs the system to execute the command without additional prompting for command confirmation.

Usage

Use this command to configure redundancy on a line card (LC) or a SPIO card. With **port-mode** enabled, if an external network device or cable failure occurs that causes a link down failure on the port, the redundant port is used.

Important: Not supported on all platforms

Important: You do not need to enter this command for each line card or SPIO card, as the system intuitively understands that if the command is entered for an active line card or SPIO card, the standby line card or SPIO card switches to operate in the same mode. For example, if you enter the **port-mode** command for an LC in slot 17, you automatically enable a redundant line card in slot 33 for port redundant operation.

Important: **asp-mode** and **port-mode** are mutually exclusive.

Example

The following command sets the redundancy mode to port redundancy.

```
redundancy port-mode
```

The following sets APS/MSP 1+1 inter-card redundancy for the specified OLC2 or CLC2 line card:

```
redundancy aps-mode
```

redundant with

Enables side-by-side (SBS) redundancy for XGLCs.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redundant with *card_number*

redundant with *card_number*

Identifies the neighboring top slot number of the card to pair with the XGLC being configured. *card_number* is an integer between 1 and 48.

Important: Attempting to use this command with any card other than an XGLC takes the card offline.

Usage

Use this command during configuration to identify the slot holding the XGLC card that will be used to provide redundancy to the XGLC you are configuring. Entering this command enables SBS redundancy when the two XGLCs occupy two upper (top) slots in a chassis.

Example

Pair the card in slot 30 with the card being configured:

```
redundant with 30
```

service-type

Configures the type of service the CLC or CLC2 line card will support.

Important: Supported in software releases 8.1 and higher.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
service-type { frame-relay | mtp2 | pwe3-cesopsn | unspecified } [ -noconfirm ]

default service-type [ -noconfirm ]
```

default

Returns the card configuration to *unspecified*.

service-type frame-relay

Configures the card to operate in Frame Relay service mode.

service-type mtp2

Important: MTP2 functionality is not yet supported.

Enables MTP2 type service to support narrowband transmissions.

service-type pwe3-cesopsn

Important: **pwe3-cesopsn** functionality has been replaced by **mtp2**.

service-type unspecified

This is the default mode for a CLC or CLC2 line card.

Important: You must configure the line card to one of the available service types or the card will not function.

-noconfirm

Executes the command without additional prompting for command confirmation.

Usage

Use this command to configure the operational service mode for the channelized line card - CLC or CLC2. Once you select the service-type, refer to the Channelized Port configuration mode chapter to review the commands needed to configure the parameters for the port.

Example

```
service-type frame-relay
```

shutdown

Configures a card for active service or terminates all processes on the card.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] shutdown
```

no

no shutdown enables the card.
Enter only the **shutdown** keyword to shut the card down.

Usage

Shut down a card to remove it from service or to enable a card to put it into service.

Important: Do not use this command to remove a card from service for maintenance. Use the command **card halt** to remove a card for service to avoid changing or deleting the active-mode configuration. See the Exec Mode chapter.

Important: Not supported on all platforms

Example

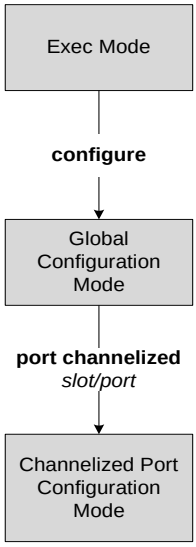
The following commands shutdown the card and switch a card to online, respectively.

```
shutdown

no shutdown
```

Chapter 48
Channelized Port Configuration Mode Commands

The channelized port configuration mode provides the commands to create, configure, bind, and manage the Frame Relay service ports on the channelized line card.

Important: Before using these commands, card framing should be configured for either SDH or SONET with the framing command described in the Card Configuration Mode chapter.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

alarm-disable

Entering this command disables the alarm detection for designated sets of alarms.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
alarm-disable { all | ds1-e1 | none | sonet-sdh }

[ no | default ] alarm-disable
```

no

Deletes the disable configuration.

default

Returns the settings for disabling alarms to the system default.

all

Disables detection of all SONET/SDH and DS1/E1 alarms.

ds1-e1

Disables detection of the DS1/E1 alarms.

none

None of the alarm detection is disabled so that all DS1/E1 and SONET/SDH alarms are detected.

sonet-sdh

Disables detection of SONE/SDH alarms.

Usage

Configure selected alarm detection for the port.

Example

Enter the following command to enable DS1/E1 and SONET/SDH alarm detection.

```
alarm-disable none
```

alarm-soak-timer

This command sets the timer for the duration that a detected alarm will be soaked before the alarm is reported.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

alarm-soak-timer *seconds*

default alarm-soak-timer

default

Returns the timer settings to the system default.

seconds

Defines the number of seconds the system waits (soaks the alarm) before reporting the alarm.
seconds: any integer from 0 to 32767.

Usage

Configures the delay before reporting detected alarms.

Example

Configure a 20 second alarm report delay.

```
alarm-soak-timer 20
```

clock-source

This command sets the source of the port's transmit clock.

Important: This command is only available for releases 8.1 or higher.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
clock-source { internal-timing | loop-timing }

default clock-source
```

default

Using this command combination sets the port clock source to internal timing.

internal-timing

Sets the port clock to derive timing from the recovered receive clock.

loop-timing

Sets the port clock to transmit in sync with the system timing.

Usage

Use this command for either SONET or SDH channelized (Frame Relay) ports on the SGSN.

Example

The following command resets the transmit clock source to internal timing.

```
default clock-source
```

description

Defines descriptive text that provides useful information about the port.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

description *text*

no description

no

Erases the port's description from the configuration file.

text

text must be a string of 1 to 79 alphanumeric characters with no spaces or a string within double quotes that includes printable characters. The description is case-sensitive.

Usage

Set the description to provide helpful information, for example the port's primary function, services, end users. Define any information, the only limit is the number of characters.

Example

description *samplePortDescriptiveText*

description *"This is a sample description"*

dlci

Identifies a data link connection identifier (DLCI), a frame relay logical connection, and binds it with a specific channelized path configuration. Once the DLCI is bound to the path, the system enters DLCI configuration mode.

Important: The **path** command must be configured prior to attempting configuration with the **dlci** command.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

dlci path *path_id* **{ ds1 | e1 }** *connects* **{ dlci** *dlci_id* **| timeslots** *slot#* **dlci** *dlci_id* **}**

no dlci path path_id { ds1 | e1 } *connects*

no

Disables the configured DLCI.

path *path_id*

Identifies a specific path configuration, set with the **path** command in this configuration mode, that will be associated with a DLCI.
path_id must be an integer from 1 to 3.

ds1 *connects* **| e1** *connects*

Selects the framing speed for the connection.
DS1: Is associated with North American networks and would be the best choice to work with the SONET framing selected with the **card** configuration command.
connects: Defines the number of logical connections supported via the DS1. The selection must be an integer from 1 to 28.
E1: is associated with European networks and would be associated with the SDH framing selected with the **card** configuration command.
connects: Defines the number of logical connections supported via the E1. The selection must be an integer from 1 to 21.

dlci *dlci_id*

Identifies a specific Frame Relay PVC DLCI to associate with the path.
dlci_id: an integer from 16 to 991.

timeslot *slot#*

Identifies one of the timeslots within a timeslot group configured with the **path** command for the E1, DS1 or fractional E1 port. Identifying one slot in a group means that all the slots in that group will have the Frame Relay parameters configured in the same manner.
slot#: Must be an integer from 1 to 31.

Usage

Associating a routing path with a specific frame relay DLCI is a significant part of the process for defining the frame relay interface.

Example

Associate path 1 with DLCI 123.

```
dlci path 1 ds1 21 dlci  123
```

end

Exits the Channelized Port configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

exit

Exits the Channelized Port configuration mode and returns to the Global configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the Global Configuration mode.

frame-relay

Configures the parameters for the Frame Relay connections for E1, DS1 and fractional E1 ports created with the **path** command. Frame

Important: The **path** command must be configured prior to attempting configuration with the **frame-relay** command.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

frame-relay path *path_id* **{ ds1** *connects* **| e1** *connects* **} timeslot** *slot#* **[intf-type** *intf_type* **] [lmi_type** *lmi_type* **]**

path *path_id*

Identifies a specific path configuration, set with the **path** command in this configuration model. *path_id* must be an integer from 1 to 3.

ds1 *connects* **| e1** *connects*

Selects the pipe splitting for the connection.
DS1: Is associated with North American networks and would be the best choice to work with the SONET framing selected with the **card** configuration command. DS1 splits the path into 28 logical connections.
connects: Defines the number of logical connections supported via the DS1. The selection must be an integer from 1 to 28.
E1: is associated with European networks and would be associated with the SDH framing selected with the **card** configuration command. E1 splits the path into 21 logical connections.
connects: Defines the number of logical connections supported via the E1. The selection must be an integer from 1 to 21.

timeslot *slot#*

Identifies one of the timeslots within a timeslot group configured with the **path** command for the E1, DS1 or fractional E1 port. Identifying one slot in a group means that all the slots in that group will have the Frame Relay parameters configured in the same manner.
slot#: Must be an integer from 1 to 31.

intf-type *intf_type*

Selecting the interface type specifies signaling parameters for the DLCI, options include:

- **dce**: Selects data circuit-terminating equipment -type signaling.
- **dte**: Selects data terminal equipment -type signaling.
- **nni**: Selects the network-to-network interface

Default: DTE for Release 8.0
Default: DCE for Release 8.1

frame-relay lmi_type *lmi_type*

Default: **none**.
Line management options include:

- **ansi** - ANSI ANNEXED LMI, may include option:
- **cisco** - Cisco/Gang Of Four LMI
- **none** - LMI Disabled
- **q933a** - Q.933A LMI

Any of the above LMI types can take one or more additional options

- **n391** *value* - Number of keep exchanges before requesting a full status message. Default is 6. *value* must be an integer from 1 to 255.
- **n392** *value* - Error Threshold value. Default is 2. *value* must be an integer from 1 to 10.
- **n393** *value* - Monitored events count value. Default is 2. *value* must be an integer from 1 to 10.
- **t391** *value* - Timer to send messages. Default is 10. *value* must be an integer from 5 to 30.
- **t392** *value* - Polling verification timer value. Default is 15. *value* must be an integer from 5 to 30.

Usage

Use this command to define LMI type and timers and to associate time group 2 with the Frame Relay connection.

Example

```
frame-relay path 1e1 3 timeslot 2
```

hopath-sdsf

Configures the high-order path for degrade/signal failure (SDSF) bit error rate (BER) thresholds.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

hopath-sdsf *hopath_value*

hopath_value

- 0: Disabled
- 1 -1.E-03
- 2 - 1.E-04
- 3 - 1.E-05
- 4 - 1.E-06
- 5 - 1.E-07
- 6 - 1.E-08
- 7 - 1.E-09
- 8 - 1.E-10

Usage

Sets a standard option for the high-order path for SDSF.
The SD is kept at a value of 100 erroredBits/sec less than the corresponding value of the SF. So if the SD threshold is configured at 1 error in every 100000 bits/sec, then the SF threshold automatically becomes 1 error in every 1000 bits/sec.

Example

```
hopath-sdsf 1
```

line-timing

This command enables the SPIO to recover transmit timing source via line attached to the selected port. By default, line-timing is not enabled.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] line-timing
```

no

Disables line-timing as the source for the transmit clock.

Usage

The port must be enabled (with the **no shutdown** command) to enable recovery of timing source via the line. As well, the card's slot number must be entered in the **recover line#** command of the BITS port configuration mode.

Example

Disable timing clock recovery on this port.

```
no line-timing
```

loopback

Configures the type of loopback mode used for diagnostic testing.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
loopback { ds1-e1-diag | ds1-e1-line | none | sonet-sdh-diag | sonet-sdh-line }
```

ds1-e1-diag

Enables a system generated diagnostic lookback signal at the DS1/E1 layer.

ds1-e1-line

Loops back a network diagnostic signal at the DS1/E1 layer.

none

Stops diagnostic loopback signalling.

sonet-sdh-diag

Enables a system generated diagnostic lookback signal at the SONET/SDH layer.

sonet-sdh-line

Loops back a network diagnostic signal at the SONET/SDH layer.

Usage

Setup diagnostic loopback signals for troubleshooting purposes.

Example

```
loopback ds1-e1-diag
```

lopath-sdsf

Configures the low-order path for signal degrade/signal failure (SDSF) bit error rate (BER) thresholds.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

lopath-sdsf *lopath_value*

lopath_value

- 0: Disabled
- 1 -1.E-03
- 10 - 1.E-12
- 2 - 1.E-04
- 3 - 1.E-05
- 4 - 1.E-06
- 5 - 1.E-07
- 6 - 1.E-08
- 7 - 1.E-09
- 8 - 1.E-10
- 9 - 1.E-11

Usage

Sets a standard option for the low-order path for SDSF.
The SD is kept at a value of 100 erroredBits/sec less than the corresponding value of the SF. So if the SD threshold is configured at 1 error in every 100000 bits/sec, then the SF threshold automatically becomes 1 error in every 1000 bits/sec.

Example

lopath-sdsf *1*

path

This command configures the parameters that define the routing path for a DLCI. It must match with the DLCI configuration parameters. The values entered with these commands should be noted as they will be needed to configure the **frame-relay** and **dlci** commands also in this configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

path *path_id* **{ ds1** *connects* **| e1** *connects* **}** *frame-mapping multiplexing index# index#* **framing** *mode* **mapping-mode { bit-sync | byte-sync } [timeslots** *slot#* **[** *slot#* **] | frame-relay [intf-type** *intf_type* **[lmi_type** *lmi_type* **]]]**

no path *path_id* **{ ds1 | e1 }***connects*

---

no

Deletes the routing path entry from the configuration.

---

path *path_id*

Identifies a specific path configuration that will be associated with a DLCI. The *path_id* must be an integer from 1 to 3.

---

ds1 *connects* **| e1** *connects*

Selects the channelization for the connection.
DS1: (AKA: T1) Is associated with North American networks and would be the best choice to work with the SONET (can also work with SDH) framing selected with the **card** configuration command. DS1 splits the path into 28 logical connections.
connects: Defines the number of logical connections supported via the DS1. The selection must be an integer from 1 to 28.
E1: is associated with European networks and would be associated with the SDH (can also work with SONET) framing selected with the **card** configuration command. E1 splits the path into 21 logical connections.
connects: Defines the number of logical connections supported via the E1. The selection must be an integer from 1 to 21.

---

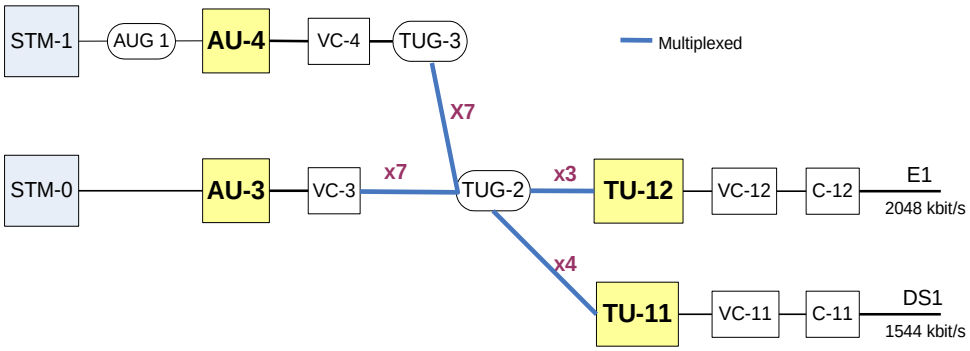
frame-mapping

Frame mapping sets the channelization according to the national standards that correlate with the framing/speed standards. This option selects the mapping of containers (C), virtual containers (VC), tributary units (TU), and tributary unit groups (TUG), that is appropriate for the channel characteristics:

- **tu11-au3**: Appropriate for DS1 in SDH. Maps as follows AU-3—VC-3— m# —TUG-2— m# —TU-12—VC-12—C-12
- **tu11-au4**: Appropriate for DS1 in SDH. Maps as follows AU-4—VC-4—TUG-3— m# —TUG-2— m# —TU-11—VC-11—C-11

- **tu12-au3**: Appropriate for E1 in SDH. Maps as follows AU-3—VC-3— m# —TUG-2— m# —TU-12—VC-12—C-12
- **tu12-au4**: Appropriate for E1 in SDH. Maps as follows AU-4—VC-4—TUG-3— m# —TUG-2— m# —TU-12—VC-12—C-12

Frame Mapping for E1 and DS1 to STM-n Interfaces



- **vt1.5**: Only appropriate for DS1 in SONET framing.
- **vt2**: Only appropriate for E1 in SONET framing.

---

multiplexing index# index#

index#: TUG-2 index - Must be an integer from 1 to 7 to identify a multiplex channel between TUG-2 and VC-3 (E1) or TUG-3 (DS1).
index#: TU index - Must be an integer from 1 to 4 (DS1) or 1 to 3 (E1) to identify a multiplex channel between TU-11 (DS1) and TUG-2 or between TU-12 (E1) and TUG-2.

---

framing *mode*

Defines the framing modes to be used for the channelization to E1 or T1 of the (optical) port.

- options for E1:
  - **cas:** standard mapping with CAS
  - **cas-crc4:** CRC4 mapping with CAS
  - **crc4:** CRC4 mapping
  - **standard:** mapping
- options for DS1:
  - **esf:** extended superframe mapping
  - **sf:** superframe mapping
  - option for either E1 or DS1:
  - **unframed**

---

mapping-mode

- **bit-sync**
- **byte-sync**

timeslots *timeslots*

Defines up to 8 timeslot groupings for multiple fractional DS1/E1 channels. Each slot is 2.048/32 Mbytes. Slots 0 and 16 are reserved for synchronization and alarms. Slots 1-15 and 17-31 are used for data. Timeslots must be unique -- a timeslot can not be used in more than one grouping.
timeslots: Must be an integer from 1 to 31. Timeslot groups are separated by spaces and can consist of a single slot and/or a range indicated with a hyphen. Example: 3,7-10 is a single fractional group. NOTE there is no space after the comma. Timeslots must be unique -- a timeslot can not be used in more than one grouping.

frame-relay

Enables definition of a Frame Relay connection with the **frame-relay** command.

Important: For release 8.1 and higher, this feature has been moved to the **frame-relay** command.

intf-type *intf_type*

Selecting the interface type specifies signaling parameters for the DLCI, options include:

- **dce**: Selects data circuit-terminating equipment -type signaling.
- **dte**: Selects data terminal equipment -type signaling.
- **nni**: Selects the network-to-network interface

Default: DTE for Release 8.0
Default: DCE for Release 8.1

Important: For release 8.1 and higher, this feature has been moved to the **frame-relay** command.

lmi_type *lmi_type*

Default: **none**.
Line management type options include:

- **ansi** - ANSI ANNEXED LMI, may include option:
- **cisco** - Cisco/Gang Of Four LMI
- **none** - LMI Disabled
- **q933a** - Q.933A LMI

Any of the above LMI types can take one or more additional options

- **n391** *value* - Number of keep exchanges before requesting a full status message. Default is 6. *value* must be an integer from 1 to 255.
- **n392** *value* - Error Threshold value. Default is 2. *value* must be an integer from 1 to 10.
- **n393** *value* - Monitored events count value. Default is 2. *value* must be an integer from 1 to 10.
- **t391** *value* - Timer to send messages. Default is 10. *value* must be an integer from 5 to 30.
- **t392** *value* - Polling verification timer value. Default is 15. *value* must be an integer from 5 to 30.

Important: For release 8.1 and higher, this feature has been moved to the **frame-relay** command.

Usage

Defines the signaling characteristics of a frame relay connection or timeslots for a fractional connection. Use this command to create E1 ports or fractional E1 ports. Fractional E1 ports are created with the timeslot definitions. The fractional E1 port can consist of one or more or all of the timeslots.

Example

In the first example, define timers for the q933a LMI-type.

```
path 1 e1 1 tu12-au4 1 1 framing crc4 mapping-mode bit-async frame-relay
intf-type dce lmi_type  q933a  n391 6 n392 2 n393 2 t391 10 t392 15
```

The next example defines 3 groups of fractional timeslots with group 1 having slots 1-5 and 8, group 2 having slot 22-25, and group 3 having slots 31.

```
path 1 e1 1 tu12-au3 1 1 framing cas  mapping-mode bit-async timeslots 1-
5,8 22-25 31
```

preferred slot

Identifies which card in a chassis should assume revertive (redundancy auto-recovery) functionality should the slot/port being configured go down. This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual LCs or SPIO cards. For example, ports 1 through 4 could be configured as "preferred" on the LC in slot 17 while ports 5 through 8 are "preferred" on the LC in slot 33. In this scenario, both LCs would be in an Active operational state while still providing LC and port redundancy for the other.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

preferred slot *slot#*

no preferred slot

slot#

Identifies the physical slot in the chassis where the line card is installed.

no

Disables revertive, or auto-recovery, operation for the port.

Usage

This command enables or disables revertive port redundancy. So after a port failover, when the original port is restored to service (i.e. link up) the system will return service to that port automatically.
Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a port switch to command to return service to the original port.

Example

```
preferred slot 17
```

pwe3-cesopsn

This command has been deprecated and replaced by the **mtp2** command.

shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, this command with the **no** keyword enables the port.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] shutdown
```

no

Enables the port's administrative state. When omitted the card is shutdown (removed from service).

Usage

Shut down a port prior to re-cabling and/or other maintenance activities.
This command with the **no** keyword is required to bring a port into service.

Example

Use the following command to disable a port:

```
shutdown
```

Use the following command to enable a port for service:

```
no shutdown
```

snmp trap link-status

Enables/disables the generation and sending of an SNMP (notification) trap when the port experiences a change of state (up or down).

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] snmp trap link-status
```

no

Disables the sending of traps for link-status changes.

Usage

Enable the sending of link-status change traps if there is a monitoring facility that can use the information or if there are troubleshooting activities in progress.

Example

```
snmp trap link-status
```

threshold high-activity

Configures the port's high and low activity thresholds.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

threshold high-activity *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 50
Sets the threshold for the highest percentage of port activity that must be met or exceeded, within the polling interval, to generate an alert or alarm.
high_thresh_% can be configured to any integer value between 0 and 100.

clear *low_thresh*

Default: 50
Sets the threshold for the lowest percentage level of port activity that must be met to generate and send a clear alarm. If port activity does not drop to or below this threshold then the alarm is maintained.
low_thresh_% can be configured to any integer value between 0 and 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

High port activity thresholds generate alerts or alarms based on the utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis.
Alerts or alarms are triggered for high port activity based on the following rules:

- **Enter condition:** Actual percent utilization of a port > High Threshold
- **Clear condition:** Actual percent utilization of a port < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the **threshold monitoring** command in this chapter to enable thresholding for this value.

Example

The following command configures a high port utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold high-activity 70 clear 50
```

threshold monitoring

Enables thresholding for port-level values.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] threshold monitoring
```

no

Disables threshold monitoring for port-level values. This is the default setting.

Usage

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high-activity) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the SNMP MIB Reference.

The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.
- **Alarm System:** High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists and/or a condition clear alarm is generated.

"Outstanding" alarms are reported to through the system's alarm subsystem and are viewable through the system's CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

Table 14. Thresholding Reporting Mechanisms by Model

Model	SNMP Traps	Logs	Alarm System
Alert	X	X	
Alarm	X	X	X

This command enables thresholding for port-level values. Refer to the **threshold high-activity**,**threshold rx-utilization**, and **threshold tx-utilization** commands in this chapter for information on configuring these values. In addition refer to the **threshold poll** command in the

Global Configuration Mode Commands chapter of this reference for information on configuring the polling interval over which these values are monitored.

Example

Use the following command to terminate thresholding:

```
no threshold monitoring
```

threshold rx-utilization

Configures thresholds for receive-port utilization.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

threshold rx-utilization *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 80
The high threshold receive port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
The percentage can be configured to any integer value between 0 and 100.

clear*low_thresh*

Default: 80
Allows the configuration of the low threshold.
The low threshold receive port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
The percentage can be configured to any integer value between 0 and 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis.

Important: Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive **or** transmit utilization threshold be configured.

Alerts or alarms are triggered for receive port utilization based on the following rules:

- **Enter condition:** Actual percent utilization of a port for received data ³ High Threshold
- **Clear condition:** Actual percent utilization of a port for received data < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the **threshold monitoring** command in this chapter to enable thresholding for this value.

Example

The following command configures a receive port high utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold rx-utilization 70 clear 50
```

threshold tx-utilization

Configures thresholds for transmit port utilization.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

threshold tx-utilization *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 80
The high threshold transmit port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
The percentage can be configured to any integer value between 0 and 100.

clear *low_thresh*

Default: 80
Allows the configuration of the low threshold.
The low threshold transmit port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
The percentage can be configured to any integer value between 0 and 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis.

Important: Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive **or** transmit utilization threshold be configured.

Alerts or alarms are triggered for transmit port utilization based on the following rules:

- **Enter condition:** Actual percent utilization of a port for transmit data ³ High Threshold
- **Clear condition:** Actual percent utilization of a port for transmit data < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the **threshold monitoring** command in this chapter to enable thresholding for this value.

Example

The following command configures a transmit port high utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold tx-utilization 70 clear 50
```

toh-sdsf

Enable/disable line SDSF BER thresholds and configure the line transport overhead (TOH) signal degrade and signal failure (SDSF) bit error rate (BER) threshold.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

toh-sdsf *toh_value*

default toh-sdsf

default

Resets the default which disables this threshold.

toh_value

To facilitate configuration the SD and SF rates have been combined into a single setting. .

- 0: Disabled
- 1 -1.E-04
- 2 - 1.E-05
- 3 - 1.E-06
- 4 - 1.E-07
- 5 - 1.E-08
- 6 - 1.E-09
- 7 - 1.E-10
- 8 - 1.E-11

Usage

This command can be used to configure the line threshold whether the port is active or standby and sets a standard option for the paired values of the line's signal degrade and signal failure (SDSF) BER.
The SD is kept at a value of 100 erroredBits/sec less than the corresponding value of the SF. So if the SD threshold is configured at 1 error in every 100000 bits/sec, then the SF threshold automatically becomes 1 error in every 1000 bits/sec.
The port will go operationally down as soon as the SD threshold is crossed.

Example

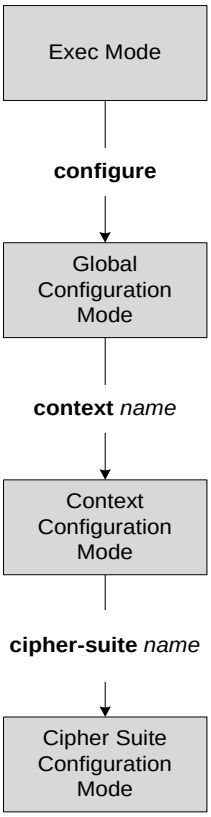
toh-sdsf *1*

vc-mapping

This command has been deprecated. Go to the **frame-mapping** keyword in the **path** command to configure this functionality.

Chapter 49
Cipher Suite Configuration Mode Commands

The Cipher Suite Configuration Mode is used to configure the building blocks for SSL cipher suites, including the encryption algorithm, hash function, and key exchange.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

encryption

Specifies the encryption algorithm for the SSL cipher suite.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
encryption { 3des | aes-128 | null | rc4 }

default encryption
```

default

Sets the encryption option to its default value of RC4.

encryption 3des | aes-128 | null | rc4

Specifies the encryption algorithm.
3des: Encryption algorithm 3DES (Triple Encryption Algorithm). 3DES applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.
aes-128: Encryption algorithm AES-128 (Advanced Encryption Standard-128). AES-128 is a symmetric-key encryption standard which has a 128-bit block size, with key size of 128.
null: Encryption algorithm Null.
rc4: Encryption algorithm RC4 (Rivest Cipher 4). RC4 is a stream cipher used with SSL protocol.

Usage

Use this command to specify encryption for the SSL cipher suite.

Example

The following command sets the encryption option to its default value, which is RC4:

```
encryption rc4
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

hmac

Specifies the HMAC (keyed-Hash Message Authentication Code) for the SSL cipher suite.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
hmac { sha1 }

default hmac
```

default

Sets the HMAC option to its default value of SHA-1.

hmac sha1

Specifies the SHA-1 (Secure Hash Algorithm-1) HMAC for the SSL cipher suite.SHA-1 uses a 160-bit secret key and produces a 160-bit digest.

Usage

Use this command to specify the SHA-1 HMAC for the SSL cipher suite. The default and only currently available option is SHA-1.
A keyed-Hash Message Authentication Code, or HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key to verify both data integrity and message authenticity.

Example

The following command sets the HMAC option to its default value, which is SHA-1:

```
hmac sha1
```

key-exchange

Specifies the key exchange algorithm for the SSL cipher suite.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
key-exchange { rsa }

default key-exchange
```

default

Sets the key exchange option to its default value of RSA.

key-exchange rsa

Specifies the RSA (Rivest, Shamir, and Adleman) key exchange algorithm for the SSL cipher suite. With RSA, the secret key is encrypted with the receiver's public key, and a public-key certificate from the receiver's key must be made available.

Usage

Use this command to specify the RSA key exchange for the SSL cipher suite. The default and only currently available option is RSA.
The key exchange algorithm provides the means by which the cryptographic keys for conventional encryption and MAC calculations are exchanged.

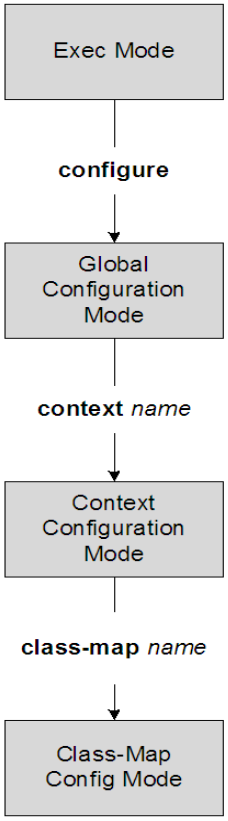
Example

The following command sets the key exchange option to its default value, which is RSA:

```
key-exchange rsa
```

Chapter 50
Class-Map Configuration Mode Commands

Class-Map is used to configure a packet classifier for the flow-based Traffic Policing feature within destination context. It filters egress and/or ingress packets of a subscriber session based on rules configured in a subscriber context.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

match any

Allows all traffic types in this class map.

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

```
match any
```

Usage

Sets the match rule to allow all traffic flow for specific class map.

Example

The following command allows all packets going to a system with this class map.

```
match any
```

match dst-ip-address

Specifies a traffic classification rule based on the destination IP address of packets.

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

match dst-ip-address *dst_ip_address* **/***subnet_mask*

match dst-ip-address *dst_ip_address*/*subnet_mask*

Specifies the destination IP address of the packets.
dst_ip_address must be entered in IPv4 dotted-decimal or IPv6 colon-separated notation.
subnet_mask is an option that is entered in CIDR notation.

Usage

Sets the match rule based on the destination IP address of packets for specific Class Map.

Example

The following command specifies the rule for packets going to a system having an IP address *10.1.2.6*.

```
match dst-ip-address 10.1.2.6
```

match dst-port-range

Specifies a traffic classification rule based on the range of destination ports for L4 packets.

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

match dst-port-range *initial_port_number* **[to** *last_port_number* **]**

match dst-port-range *initial_port_number* **[to** *last_port_number* **]**

Specifies the destination port or range of ports of L4 packets.
initial_port_number is the starting port number and must be an integer 1 to 65535 but less than *last_port_number*, if specified.
last_port_number is the end port number and must be an integer from 1 to 65535 but more than *initial_port_number*.

Usage

Sets the match rule based on the destination port number or range of ports of L4 packets for specific Class Map.

Example

The following command specifies the rule for packets having destination port number from *23* to *88*.

```
match dst-port-range 23 to 88
```

match ip-tos

Specifies a traffic classification rule based on the IP Type of Service value in ToS field of packet.

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Administrator

Syntax

match ip-tos { *service_value* [ip-tos-mask *mask_value*] | tos-range *low_value* to *high_value* }

---

match ip-tos *service_value*

Specifies the IP Type-of-Service value to match inside the ToS field of packets as an integer from 0 to 255.

---

ip-tos-mask *mask_value*

Specifies the IP Type-of-Service mask value to match inside the ToS field of packets as an integer from 1 to 255.

---

tos-range *low_value* to *high_value*

Specifies a range that a ToS value in a received packet must fall within to be considered a match. *low_value* and *high_value* must be an integer from 0 to 255.

Usage

Sets the match rule based on the IP ToS value in ToS field of packets for specific Class Map.

Example

The following commands specifies the IP ToS value of *3* is the value to match in a ToS field in received packets.

```
match ip-tos 3
```

match ipsec-spi

Specifies a traffic classification rule based on the IPSec Security Parameter Index (SPI) value in the SPI field of packet.

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

match ipsec-spi *index_value*

match ipsec-spi *index_value*

Specifies the IPSec SPI value to match inside the SPI field of packets as an integer from 1 to 65535.

Usage

Sets the match rule based on the IPSec SPI value in SPI field of packets for specific Class Map.

Example

The following command specifies the IPSec SPI value as *1234* for the SPI field in packets.

```
match ipsec-spi 1234
```

match packet-size

Specifies a traffic classification rule based on the size of packet.

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

match packet-size [gt | lt] *size*

match packet-size [gt | lt] *size*

Specifies the packet length in bytes.
gt: indicates a packet size greater than the specified size.
lt: indicates a packet size less than the specified size.
size must be an integer from 1 to 65535.

Usage

Sets the match rule based on the size of packets for specific Class Map. This command is only applicable for static policies; it is not available for dynamic policies.

Example

The following command specifies the packet length to be *1024* bytes.

```
match packet-size 1024
```

match protocol

Specifies a traffic classification rule based on the protocol used for session flow.

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

```
match protocol { gre | ip-in-ip | number | rtp | sip | tcp | udp }
```

match protocol gre

Sets the match rule for session flow using Generic Routing Encapsulation (GRE) Protocol. It matches the protocol field to GRE inside the packet.

match protocol ip-in-ip

Sets the match rule for session flow using IP-in-IP encapsulation protocol. It matches the protocol field to ip-in-ip inside the packet.

match protocol number

Sets the match rule for a session flow using Transmission Control Protocol (TCP). It matches the specified protocol field inside the packet.

match protocol rtp

Sets the match rule for a session flow using Real Time Protocol (RTP). It matches the specified protocol field inside the packet.

match protocol sip

Sets the match rule for a session flow using Session Initiation Protocol (SIP). It matches the specified protocol field inside the packet.

match protocol tcp

Sets the match rule for a session flow using Transmission Control Protocol (TCP). It matches the protocol field to TCP inside the packet.

match protocol udp

Sets the match rule for a session flow having User Datagram Protocol (UDP). It matches the protocol field to UDP inside the packet.

Usage

Sets the match rule based on the protocol of packet flow for a specific Class Map.

Example

The following command specifies the rule for packet flow using IP-in-IP protocol.

```
match protocol ip-in-ip
```

match src-ip-address

Specifies a traffic classification rule based on the source IP address of packets.

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

match src-ip-address *src_ip_address* **/***subnet_mask*

match src-ip-address *src_ip_address*/*subnet_mask*

Specifies the destination IP address of the packets.
src_ip_address must be entered in IPv4 dotted-decimal or IPv6 colon-separated notation.
subnet_mask is an option that is entered in CIDR notation.

Usage

Sets the match rule based on the source IP address of packets for specific Class Map.

Example

The following command specifies the rule for packets coming from a system having an IP address *10.1.2.3*.

```
match src-ip-address 10.1.2.3
```

match src-port-range

Specifies a traffic classification rule based on the range of source ports of L4 packets.

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

match src-port-range *initial_port_number* **[to** *last_port_number* **]**

initial_port_number **[to** *last_port_number* **]**

Specifies the source port or range of ports of the L4 packets.
initial_port_number is the starting port number and must be an integer from 1 to 65535 but less than *last_port_number*, if specified.
last_port_number is the end port number and must be an integer from 1 to 65535 but more than *initial_port_number*.

Usage

Sets the match rule based on source port number or range of ports of L4 packets for specific Class Map.

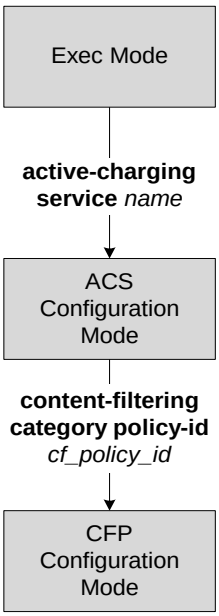
Example

The following command specifies the rule for packets having source port number from *23* to *88*.

```
match src-port-range 23 to 88
```

Chapter 51
Content Filtering Policy Configuration Mode Commands

The Content Filtering Policy Configuration Mode allows you to configure analysis and action when Content Filtering (CF) matches a Content Filtering Category Policy Identifier.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

analyze

Specifies the action to take for the indicated result after content filtering analysis.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

In 12.1 and earlier releases:

```
analyze priority priority { all | category category | x-category string } action { allow
| content-insert content_string | discard | redirect-url url | terminate-flow | www-
reply-code-and-terminate-flow reply_code } [ edr edr_format_name ]

no analyze priority priority
```

In 12.2 and later releases:

```
analyze priority priority { all | category category | x-category string } action { allow
| content-insert content_string | discard | redirect-url url | terminate-flow | www-
reply-code-and-terminate-flow reply_code } [ reporting-edr reporting_edr_format_name ]

no analyze priority priority
```

---

no

Removes the specified analyze priority configuration.

---

priority *priority*

Specifies the precedence of a category in the content filtering policy.
priority must be an integer from 1 to 65535 that is unique in the content filtering policy.

---

all

Specifies the default action to take if the category returned after rating is not configured in the subscriber's content filtering policy. This has the lowest priority.

---

category *category*

Specifies the category.
category must be one of the following.

- ABOR
- ADULT
- ADVERT
- ANON
- ART
- AUTO
- BACKUP

- BLACK
- BLOG
- BUSI
- CAR
- CDN
- CHAT
- CMC
- CRIME
- CULT
- DRUG
- DYNAM
- EDU
- ENERGY
- ENT
- FIN
- FORUM
- GAMB
- GAME
- GLAM
- GOVERN
- HACK
- HATE
- HEALTH
- HOBBY
- HOSTS
- KIDS
- LEGAL
- LIFES
- MAIL
- MIL
- NEWS
- OCCULT
- PEER
- PERS
- PHOTO
- PLAG
- POLTIC

- PORN
- PORTAL
- PROXY
- REF
- REL
- SCI
- SEARCH
- SHOP
- SPORT
- STREAM
- SUIC
- SXED
- TECH
- TRAV
- VIOL
- VOIP
- WEAP
- WHITE
- UNKNOW

Important: Content can simultaneously match multiple categories, therefore specific **priority** must be used for required evaluation precedence.

x-category *string*

This keyword can be used to configure runtime categories not present in the CLI.
string specifies the unclassified category to be rated, and must be an alphanumeric string of 1 through 6 characters.
A maximum of 10 x-categories can be configured.

action { allow | content-insert *content_string* **| discard | redirect-url** *url* **| terminate-flow | www-reply-code-and-terminate-flow** *reply_code* **}**

Specifies the action to take for the indicated result of content filtering analysis.
allow: With static content filtering, this option allows the request for content. In dynamic content filtering it allows the content itself.
content-insert *content_string*: Specifies the content string to be inserted in place of the message returned from prohibited/restricted site or content server.
For static content filtering, *content_string* is used to create a response to the subscriber's attempt to get content. In dynamic content filtering, it is used to replace the content returned by a server.
content_string must be an alphanumeric string of 1 through 1023 characters.
discard: For static content filtering, this option discards the packet(s) that requested. In dynamic content filtering, it discards the packet(s) that contain(s) the content.
redirect-url *url*: Redirects the subscriber to the specified URL.

url must be an alphanumeric string of 1 through 1023 characters in the *http://search.com/subtarg=#HTTP.URL#* format.
terminate-flow: Terminates the TCP connection gracefully between the subscriber and server, and sends a TCP FIN to the subscriber and a TCP RST to the server.
www-reply-code-and-terminate-flow *reply_code*: Terminates the flow with the specified reply code. *reply_code* must be a reply code that is an integer from 100 through 599.

Important: Static-and-Dynamic Content Filtering is only supported in 9.0 and later releases.

edr *edr_format_name*

Important: This option is applicable only to 12.1 and earlier releases. In 12.2 and later releases, it is deprecated and replaced by the **reporting-edr** option.

Generates separate EDRs for content filtering based on action and content category using a specified EDR file format name.
edr_format_name is the name of a pre-defined EDR file format name in the EDR Format Configuration Mode, and must be an alphanumeric string of 1 through 63 characters.

Important: EDRs generated through this keyword are different from charging EDRs generated for subscriber accounting and billing. For more information on generation of charging EDRs, refer to the *ACS Rulebase Configuration Mode Commands* chapter.

reporting-edr *reporting_edr_format_name*

Important: This option is available only in 12.2 and later releases.

Generates separate reporting EDRs for Content Filtering based on the action and content category using the specified EDR file format name.
reporting_edr_format_name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify the action and priorities for the indicated result of content filtering analysis. Up to 64 priorities and actions can be entered with this command.

Example

The following command sets priority *10* for category *ADULT* with action as **terminate-flow**:

```
analyze priority 10 category ADULT action terminate-flow
```

discarded-flow-content-id

Accounts for packets discarded as a result of content filtering action.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

discarded-flow-content-id *content_id*

no discarded-flow-content-id

content_id

Specifies the content ID for discarded flows as an integer from 1 through 65535.

Usage

Use this command in the configuration to account for packets discarded as a result of CF action.
A flow end-condition EDR would be generated as a charging EDR for content-filtered packets. No billing EDRs (even with flow-end) would be generated for a discarded packet as the flow will not end. Dual EDRs would exist for customers who want to use "flow end" to get EDRs for charging, plus CF-specific EDRs. The second EDR for charging comes from the **flow end-condition content-filtering** configuration in the Rulebase Configuration Mode.
The **discarded-flow-content-id** configuration can be used for accumulating statistics for UDR generation in case CF discards the packets. These statistics for UDR generation (based on the CF content ID) would also be accumulated in case of ACS error scenarios where the packets are discarded but the flow does not end.
If, in the Rulebase Configuration Mode, the **content-filtering flow-any-error** configuration is set to **deny**, then all the denied packets will be accounted for by the **discarded-flow-content-id** config. That is, the *content_id* will be used to generate UDRs for the denied packets in case of content filtering.

Example

Use the following command to set the accumulation of statistics for UDR generation based on the CF content ID *1003*:

```
discarded-flow-content-id 1003
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

failure-action

Specifies the failure action when the content filtering analysis results are not available to analyze.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

```
failure-action { allow | content-insert content_string | discard | redirect-url url |
terminate-flow | www-reply-code-and-terminate-flow reply_code } [ edr edr_format_name ]

default failure-action [ edr edr_format_name ]
```

default

Configures the default setting of discard.

allow

In static content filtering, this option allows the request for content. In dynamic content filtering it allows the content itself.

Important: Static-and-Dynamic Content Filtering is only supported in 9.0 and later releases.

content-insertion *content_string*

Specifies the content string to be inserted in place of the message returned from the content server due to connection timeout or when no category policy ID is available for the content.
For content filtering, the *content_string* is used to create a response to the subscriber's attempt to get content. In dynamic content filtering it replaces the content returned by a server.
content_string is an alphanumeric string of 1 through 1023 characters.

Important: Static-and-Dynamic Content Filtering is only supported in 9.0 and later releases.

discard

In static content filtering, specifies discarding the packet(s) that requested. In dynamic content filtering it discards the packet(s) that contain the content.

Important: Static-and-Dynamic Content Filtering is only supported in 9.0 and later releases.

redirect-url *url*

Redirects the subscriber to the specified URL.
url must be an alphanumeric string of 1 through 1023 characters, in the following format:
http://search.com/subtarg=#HTTP.URL#

terminate-flow

Terminates the TCP connection gracefully between the subscriber and external server and sends a TCP FIN to the subscriber and a TCP RST to the server.

www-reply-code-and-terminate-flow *reply_code*

Sets action as terminate-flow with a reply code that is a 3-digit integer from 100 through 599.

edr *edr_format_name*

Specifies the name of a pre-defined EDR format to be generated on the content filtering action as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to set the failure action to take when no content filtering analysis result is available to analyze for **analyze priority** *priority* **category** *category_string* command.

Example

The following command sets the failure action as **discard**:

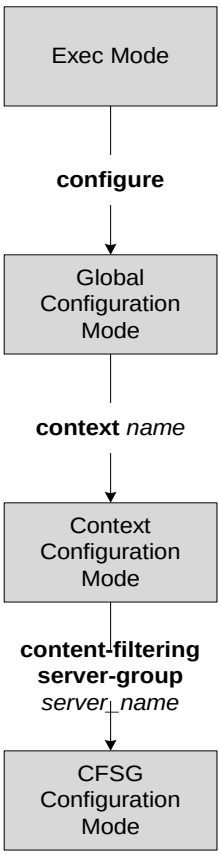
```
failure-action discard
```

timeout action

This command has been deprecated, and is replaced by the failure-action command.

Chapter 52
Content Filtering Server Group Configuration Mode Commands

Content Filtering Server Group Configuration Mode sets the parameters for interoperating with a group of external servers. It is accessed by entering the **`content-filtering server-group`** command in the Context Configuration Mode.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

connection retry-timeout

Configures the TCP connection retry timer for Internet Content Adaptation Protocol (ICAP) server and client.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

connection retry-timeout *duration*

{ default | no } connection retry-timeout

default

Configures the default setting of 30 seconds.

no

Removes the connection retry timeout configuration.

duration

Specifies the duration (in seconds) as an integer from 1 to 3600. Default: 30

Usage

Use this command to configure the connection retry timer between ICAP server and client TCP connection, i.e. how long to wait before re-attempting to establish a TCP connection.

Example

The following command sets the ICAP client and server connection retry timer to 120 seconds:

```
connection retry-timeout 120
```

deny-message

Configures the text message that is returned to the subscriber in a deny response.

Important: This command is obsolete in 10.0 and later releases.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

deny-message *string*

{ default | no } deny-message

default

Configures the default setting of Disabled.

no

Removes previously configured deny message setting.

string

Specifies a text message that is to be returned to the subscriber in a deny response as an alphanumeric string of 1 through 511 characters.

Usage

Use this command to define a text message that is returned to the subscriber in a deny response.

Example

The following command sets the text message to *no_Authorization* in a deny message:

```
deny-message no_Authorization
```

deny-response code

Configures the deny response message that is to be sent from the ICAP server to the subscribers.

Product

ICAP

Privilege

Security Administrator, Administrator

Syntax

```
deny-response code { 200 message string | 403 }

{ default | no } deny-response code
```

default

Configures the default setting of **deny-response code 200**.

no

Removes previously configured deny response message setting.

deny-response code 200 message *string*

Specifies a text message that is to be returned to the subscriber in a code 200 deny response. as an alphanumeric string of 1 through 511 characters.
If **deny-response code 200** is configured, the response sent to the subscriber will be of the form 200 OK with deny messages denied. If a message is configured for response code 200, that message will be used instead of "Access denied".

deny-response code 403

This keyword is used to set response code 403 for the deny response message.
When this keyword is configured, the deny response from the ICAP server will be sent “as is” to the subscriber.

Usage

Use this command to define a text message that is returned to the subscriber in a deny response.

Example

The following command sets the text message to *Not allowed* in a deny response message:

```
deny-response code 200 message Not allowed
```

dictionary

Specifies the dictionary to use for requests to the server(s) in this Content Filtering Server Group (CFSG).

Product

CF

Privilege

Security Administrator, Administrator

Syntax

```
dictionary { custom1 | custom2 | standard }

{ default | no } dictionary
```

default

Sets the default dictionary.
Default: **default**

no

Removes the previously configured dictionary setting.

custom1

Specifies a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99. It provides proprietary header fields for MSISDN and APN/subscriber. Please contact your local Cisco representative for more information.

custom2

Custom-defined dictionary. Please contact your local Cisco representative for additional information.

standard

Default: Enabled
This dictionary uses an HTTP Get Request to specify the URL. It conforms to TS 32.215 v 4.6.0 for R4 (and also R5 - extended QoS format).

Usage

Use this command to specify the standard and customized encoding mechanism used for elements included messages.

Example

The following command configures the system to use standard dictionary to encode messages:

```
default dictionary
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

failure-action

Specifies the actions to be taken when communication between ICAP endpoints within this Content Filtering Server Group (CFSG) fail.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

failure-action { allow | content-insertion *content_string* **| discard | redirect-url** *url* **| terminate-flow }**

{ default | no } failure-action

default

Configures the default setting of **terminate-flow**.

no

Removes previously configured failure action.

allow

For static content filtering, this option allows the request for content. In dynamic content filtering, it allows the content itself.

content-insertion *content_string*

Specifies the content string to be used for failure action.
For static content filtering, the specified text is used to create a response to the subscriber's attempt to get content. In dynamic content filtering, the specified text replaces the content returned by a server.
content_string must be an alphanumeric string of 1 through 128 characters.

discard

For static content filtering, this option discards the packet(s) requested. In dynamic content filtering, it discards the packet(s) that contain(s) the content.

redirect-url *url*

Redirects the subscriber to the specified URL.
url must be an alphanumeric string of 1 through 128 characters in the following format:
http://search.com/subtarg=#HTTP.URL#

terminate-flow

For TCP, gracefully terminates the connection between the subscriber and external server, and sends a TCP FIN to the subscriber and a TCP RST to the server.

For WAP-Connection Oriented, the WSP session is gracefully terminated by sending WTP Aborts for each of the outstanding requests, and WSP Disconnect to the client and the server. For WSP-Connectionless, only the current WSP request is rejected.

Usage

Use this command to set the actions on failure for server connection.
ICAP rating is enabled for retransmitted packets when the default ICAP failure action was taken on an ICAP request for that flow. ICAP default failure action is taken on the pending ICAP request for a connection when the connection needs to be reset and there is no other redundant connection available. For example, in the ICAP request timeout and ICAP connection timeout scenarios, the retransmitted packet in the uplink direction is sent for ICAP rating again.
For WAP CO, uplink retransmitted packets for the WAP transactions for which ICAP failure action was taken will be sent for ICAP rating. The WSP header of the retransmitted packet is not parsed by the WSP analyzer. The URL received in the previous packet for that transaction is used for ICAP rating. If failure action was taken on multiple WTP transactions for the same flow (case: WTP concatenated GET request), the uplink retransmitted packet for each of the transactions is sent for rating again.
For HTTP, uplink retransmitted packets for the HTTP flow on which ICAP failure action is taken are sent for ICAP rating. The URL present in the current secondary session (last uplink request) is used for ICAP rating. However, if there were multiple outstanding ICAP requests for the same flow (pipelined request), the retransmitted packet for the URL sent for rating will be that of the last GET request.
Retransmission in various cases of failure-action taken on retransmitted packets when the ICAP response is not received for the original request and the retransmitted request comes in:

- WSP CO:
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked. It is possible that the WAP gateway sends the response for the permitted GET request. Hence, there is a race condition and the subscriber may be able to view the web page even thought the rating was redirect or content insert.
  - Content Insert: The retransmitted packet is not sent for ICAP rating.
  - Redirect: The retransmitted packet is not sent for ICAP rating.
  - Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked.
  - Terminate flow: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed or blocked. The WAP gateway may send an Abort transaction for this GET request if the WSP disconnect packet sent while terminating the flow is received by the WAP gateway.
- HTTP:
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the last HTTP GET request. It is possible that the HTTP server sends the response for the permitted GET request. Hence there is a race condition and the subscriber may be able to view the web page even thought the rating was redirect or content insert.
  - Content Insert: Retransmitted packets are dropped and not charged.
  - Redirect: Retransmitted packets are dropped and not charged.
  - Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction allowed/blocked.
  - Terminate flow: Retransmitted packets will be dropped and not charged.

Example

The following command sets the failure action to terminate:

```
failure-action terminate-flow
```

icap server

Adds an Internet Content Adaptation Protocol (ICAP) server configuration to the current Content Filtering Server Group (CFSG).

Important: In 8.1 and later releases, a A maximum of five ICAP servers can be configured per Content Filtering Server Group. In 8.0 and earlier releases, only one ICAP Server can be configured per Content Filtering Server Group.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

icap server *ip_address* **[port** *port_number* **] [max** *messages* **] [priority** *priority* **]**

no icap server *ip_address* **[port** *port_number* **] [priority** *priority* **]**

no

Removes the specified ICAP server configuration from the current Content Filtering Server Group.

ip_address

Specifies the ICAP server's IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.

port *port_number*

Specifies the ICAP server's port number to use for communications as an integer from 1 to 65535. Default: 1344

max *messages*

Specifies the maximum number of unanswered outstanding messages that may be allowed to the ICAP server as an integer from 1 to 4096. Default: 256

Important: The maximum outstanding requests per ICAP connection is limited to one. Therefore the value configured using the **max** keyword will be ignored.

priority *priority*

Specifies priority of the ICAP server in the current Content Filtering Server Group. The priority is used in server selection to determine which standby server becomes active. *priority* must be an integer from 1 (highest priority) to 65535 (lowest priority). Default: 1

Important: The **priority** keyword is only available in 8.1 and later releases.

Usage

This command is used to add an ICAP server configuration to a Content Filtering Server Group with which the system is to communicate for content filtering communication.
In 8.0, the ICAP solution supports only one connection between ACS Manager and ICAP server.
In 8.1, multiple ICAP server connections are supported per manager. At any time only one connection is active with the other connections acting as standby. In case of a connection failure, based on its priority, a standby connection becomes active. Any pending ICAP requests are moved to the new active connection. If a standby connection is unavailable, failure action is taken on all pending ICAP requests. See the failure-action command.
In 8.1 and later releases, a maximum of five ICAP servers can be configured per Content Filtering Server Group with a priority associated with each server. Once configured, an ICAP server's priority cannot be changed. To change a server's priority, the server configuration must be removed, and added with the new priority.

Example

The following command sets the ICAP server IP address to *10.2.3.4* and port to *1024*:

```
icap server 10.2.3.4 port 1024
```

The following command specifies an ICAP server with IP address *10.6.7.8*, port number *1024*, and priority *3*:

```
icap server 10.6.7.8 port 1024 priority 3
```

origin address

Specifies a bind address for the Content Filtering Server Group (CFSG) endpoint.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

origin address *ip_address*

no origin address

no

Disables/releases the binding address for the CFSG endpoint.

ip_address

Specifies the IP address to bind the CFSG endpoint in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to set the bind address for the CFSG endpoint.

Example

The following command sets the origin address of *10.1.1.1*:

```
origin address 10.1.1.1
```

response-timeout

Sets the response timeout for the ICAP connection between the ICAP server and client.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

response-timeout *duration*

{ default | no } response-timeout

default

Configures the default setting of 30 seconds.

no

Removes the response timeout configuration.

duration

Specifies the timeout duration (in seconds) as an integer from 1 to 300. Default: 30

Usage

Use this command to set the ICAP connection response timeout, after which connection will be marked as unsuccessful between ICAP endpoint.

Example

The following command sets the ICAP connection response timeout to *100* seconds:

```
response-timeout 100
```

timeout action

This command has been deprecated, and is replaced by the failure-action command.

url-extraction

Enables configuration of ICAP URL extraction behavior.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

```
url-extraction { after-parsing | raw }

default url-extraction
```

default

Configures the default setting of **after-parsing**.

after-parsing

Specifies sending the parsed URI and host name. Percent-encoded hex characters in URLs sent from the ACF client to the ICAP server will be converted to corresponding ASCII characters before being sent.
For example, the URL: *http://www.google.co.uk/?this%20is%20a%20test* will be sent to the ICAP server as:
http://www.google.co.uk/?this is a test

raw

Specifies sending raw URI and host name. The URLs will contain percent-encoded hex characters "as is".
For example, the URL *http://www.google.co.uk/?this%20is%20a%20test* will be sent to the ICAP server as:
http://www.google.co.uk/?this%20is%20a%20test

Usage

Use this command to configure the ICAP URL extraction behavior. Percent-encoded hex characters—for example, space (%20) and the percent character (%25)—in URLs sent from the ACF client to the ICAP server can be sent either as percent-encoded hex characters or as their corresponding ASCII characters.

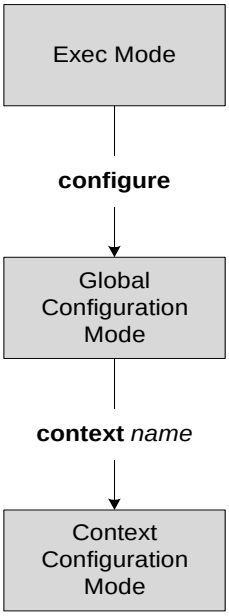
Example

The following command configures URLs sent from the ACF client to the ICAP server to contain the escape encoding as is:

```
url-extraction raw
```

Chapter 53
Context Configuration Mode Commands

The Context Configuration Mode is used to create and manage contexts in the system. Contexts facilitate management of subscribers and services in the system.



aaa accounting

This command enables/disables accounting for subscribers and context-level administrative users for the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
aaa accounting { administrator radius-diameter | subscriber [ radius-diameter ] }

default aaa accounting { administrator | subscriber }

no aaa accounting { administrator | subscriber } [ radius-diameter ]
```

default

Configures the default setting.
Default: RADIUS

no

Disables AAA accounting per the options specified.

radius-diameter

Enables AAA accounting for context-level administrative users.

subscriber

Enables AAA accounting for subscribers.

radius-diameter

Enables RADIUS or Diameter accounting for subscribers.

Usage

Use this command to enable/disable accounting for subscribers and context-level administrative users for the current context.
To enable or disable accounting for individual local subscriber configurations refer to the **accounting-mode** command in the *Subscriber Configuration Mode Commands* chapter.

Important: The accounting parameters in the APN Configuration Mode take precedence over this command for subscriber sessions. Therefore, if accounting is disabled using this command but enabled within the APN configuration, accounting is performed for subscriber sessions.

Example

The following command disables AAA accounting for context-level administrative users:

```
no aaa accounting administrator
```

The following command enables AAA accounting for context-level administrative users:

```
aaa accounting administrator radius-diameter
```

aaa authentication

This command enables/disables authentication for subscribers and context-level administrative users for the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] aaa authentication { administrator | subscriber } { local | none | radius-diameter }
```

```
default aaa authentication { administrator | subscriber }
```

default

Configures the default setting for the specified parameter.

- **administrator**: local+RADIUS
- **subscriber**: RADIUS

no

Disables AAA authentication for administrator(s)/subscribers as specified.

- **local**: Disables local authentication for current context.
- **none**: Disables NULL authentication for current context, which enables both local and RADIUS-based authentication.
- **radius-diameter**: Disables RADIUS or Diameter-based authentication.

administrator | subscriber

- **administrator**: Enables authentication for administrative users.
- **subscriber**: Enables authentication for subscribers.

local | none | radius-diameter

Enables AAA authentication for administrator(s)/subscribers as specified.

- **local**: Enables local authentication for the current context.
- **none**: Disables authentication for the current context.
- **radius-diameter**: Enables RADIUS or Diameter-based authentication.

Usage

Use this command to enable/disable AAA authentication during specific maintenance activities or during test periods. The authentication can then be enabled again for the entire context as needed.

Example

The following command disables RADIUS or Diameter-based authentication for subscribers for the current context:

```
no aaa authentication subscriber radius-diameter
```

The following command enables RADIUS or Diameter-based authentication for subscribers for the current context:

```
aaa authentication subscriber radius-diameter
```

aaa constructed-nai

This command configures the password used during authentication for sessions using a Constructed Network Access Identifier (NAI) or an APN-specified user name.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

aaa constructed-nai authentication [[encrypted] password *user_password* **| use-shared-secret-password]**

no aaa constructed-nai authentication

no

Disables authentication based upon the constructed NAI.

[encrypted] password *user_password*

encrypted: Specifies that the user password should be encrypted.
password *user_password*: Specifies an authentication password for the NAI-constructed user.
In 12.1 and earlier releases, the *user_password* must be an alphanumeric string of 0 through 63 characters with or without encryption.
In 12.2 and later releases, the *user_password* must be an alphanumeric string of 0 through 63 characters without encryption, or 1 through 132 characters with encryption.

use-shared-secret-password

Specifies using RADIUS shared secret as the password. Default: No password

Usage

This command configures passwords for user sessions that utilize a constructed NAI assigned via a PDSN service or a user name assigned via the APN configuration.
For simple IP sessions facilitated by PDSN services in which the **authentication allow-noauth** and **aaa constructed-nai** commands are configured, this command provides a password used for the duration of the session.
For PDP contexts using an APN in which the outbound user name is configured with no password, this command is used to provide the password. Additionally, this command is also used to provide a password for situations in which an outbound username and password are configured and the **authentication imsi-auth** command has been specified.
The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.
If a password is configured with this keyword, then the specified password is used. Otherwise, an empty user-password attribute is sent.

Note that this configuration works in a different way for GGSN services. If a password is configured with this keyword for GGSN service, the specified password is used. Otherwise, if an outbound password is configured, that password is used. If no outbound password is configured, the RADIUS server secret is used as the user-password string to compute the user-password RADIUS attribute.
The NAI-construction consists of the subscriber's MSID, a separator character, and a domain. The domain that is used is either the domain name supplied as part of the subscriber's user name or a domain alias.

Important: The domain alias can be set with the **nai-construction domain** command in the PDSN Service Configuration mode, or the **aaa default-domain subscriber** command in the Global Configuration mode for other core network services.

The domain alias is determined according to the following rules:

- If the domain alias is set by **nai-construction domain**, that value is always used and the **aaa default-domain subscriber** value is disregarded, if set. The NAI is of the form **<msid><symbol><nai-construction domain>**.
- If the domain alias is not set by **nai-construction domain**, and the domain alias is set by **aaa default-domain subscriber**, the **aaa default-domain subscriber** value is used. The NAI is of the form **<msid><symbol><aaa default-domain subscriber>**.
- If the domain alias is not set by **nai-construction domain** or **aaa default-domain subscriber**, the domain name alias is the name of the source context for the PDSN service. The NAI is of the form **<msid><symbol><source context of PDSN Service>**.

The special separator character can be one of the following six: @, -, %, \, -, /
The subscriber's MSID is constructed in one of the formats displayed in the following figure.

Mobile Country Code (3 digits)	Mobile Network Code (2 or 3 digits)	Mobile Subscriber Identification Number (10 digits max)

International Mobile Station Identity (IMSI)

Area Code (3 digits)	Office Code (3 digits)	Subscriber Number (4 digits)

Mobile Identification Number (MIN)

Mobile Country Code (3 digits)	Mobile Network Code (1 digit)	Subscriber Number (6 digits)

International Roaming MIN (IRM)

Example

The following command configures the authentication password for the NAI-constructed user.

```
aaa constructed-nai authentication
```

aaa filter-id rulebase mapping

This command configures the system to use the value of the Filter-Id AVP as the ACS rulebase name.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] aaa filter-id rulebase mapping
```

no

Disables the mapping of Filter-Id AVP and ACS rulebase name.

default

Configures the default setting. Default: Disabled

Usage

Use this command to enable the mapping of Filter-Id attribute's value returned during RADIUS authentication as the ACS rulebase name.
This feature provides the flexibility for operator to transact between multi-charging-service support for postpaid and prepaid subscribers through Access Control Lists (ACLs) entered in AAA profiles in RADIUS server to single-charging-service system based on rulebase configuration for postpaid and prepaid subscribers.
This feature internally maps the received ACL in to rulebase name and configures subscriber for postpaid or prepaid services accordingly.
When this feature is enabled and ACS rulebase attribute is not received from RADIUS or not configured in local default subscriber template system copies the filter-id attribute value to ACS rulebase attribute.
This copying happens only if the filter-id is configured and received from RADIUS server and ACS rulebase is not configured in ACS or not received from RADIUS.

Example

The following command enables the mapping value of the Filter-Id attribute to ACS rulebase name:

```
aaa filter-id rulebase mapping
```

aaa group

This command enables/disables the creation, configuration or deletion of AAA server groups in the context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

aaa group *group_name* **[-noconfirm]**

no aaa group *group_name*

no

Deletes the specified AAA group.

group_name

Specifies name of the AAA group.
If the specified AAA group does not exist, it is created, and the prompt changes to the AAA Server Group Configuration Mode, wherein the AAA group can be configured.
If the specified AAA group already exists, the prompt changes to the AAA Server Group Configuration Mode, wherein the AAA group can be configured.
group_name must be an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any prompt and confirmation from the user.

Usage

Use this command to create/configure/delete AAA server groups within the context. Also, refer to the *AAA Server Group Configuration Mode Commands* chapter.

Example

The following command enters the AAA Server Group Configuration Mode for a AAA group named *test321*:

```
aaa group test321
```

aaa nai-policy

This command sets policies on how Network Access Identifiers (NAIs) are handled during the authentication process.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] aaa nai-policy reformat-alg-hex-0-9
```

default

Sets the NAI policy back to its default setting which is to remap hexadecimal digits in NAIs and accept calls with embedded 0x00 hexadecimal digits.

no

Disable remapping of hexadecimal digits in the NAI and reject calls that have a 0x00 hexadecimal digit embedded in the NAI.

reformat-alg-hex-0-9

Default: Enabled
Controls remapping of NAIs that consist only of hex digits 0x00 through 0x09 or if a 0x00 hexadecimal digit is embedded in the NAI.
By default, the system remaps NAIs that consist solely of characters 0x00 through 0x09 to their ASCII equivalent. For example; 0x00 0x01 0x2 0x03 will get remapped to 123.
Also by default the system accepts an NAI containing one or more 0x00 characters within the NAI ignoring all characters after the first 0x00.
When this keyword is disabled NAIs are processed as follows:

- Remapping of hexadecimal digits 0x00 through 0x09 within the user-provided NAI is disabled.
- When the NAI has an embedded 0x00 character anywhere within it (including if there is an extra 0x00 character at the end) the call is rejected.

Usage

Use this command to disable or re-enable remapping of hexadecimal digits in the NAI.

Example

The following command disables the remapping of hexadecimal digits in the NAI:

```
no aaa nai-policy reformat-alg-hex-0-9
```

access-list undefined

Configures the behavior of access control for the current context when an undefined access control list is specified.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
access-list undefined { deny-all | permit-all }

{ default | no } access-list undefined
```

default

Configures the default setting.

no

Disables handling undefined access lists.

access-list undefined deny-all

Specifies to drop all packets when an undefined ACL is specified.

access-list undefined permit-all

Specifies to forward all packets when an undefined ACL is specified.

Usage

Use this command to specify the default behavior when an ACL specified does not exist.
When the security policies require strict access control the **deny-all** handling should be configured.

Example

The following command sets the packet handling to ignore (drop) all packets when an undefined ACL is specified.

```
access-list undefined deny-all
```

administrator

Configures a user with Security Administrator privileges in the current context.

Product

All

Privilege

Security Administrator

Syntax

administrator *user_name* **[encrypted] password** *password* **| [ecs] [expiry-date** *date_time* **] [ftp] [li-administration] [nocli] [noecs] [timeout-absolute** *timeout_absolute* **] [timeout-min-absolute** *timeout_min_absolute* **] [timeout-idle** *timeout_idle* **][timeout-min-idle** *timeout_min_idle* **]**

no administrator *user_name*

---

no

Removes Security Administrator privileges for the specified user name.

---

administrator *user_name*

Specifies the user name for which Security Administrator privileges must be enabled in the current context. *user_name* must be an alphanumeric string of 1 through 32 characters.

[encrypted] password *password*

Specifies password for the user name. Optionally, the **encrypted** keyword can be used to specify the password uses encryption.
password must be an alphanumeric string of 1 through 63 characters without encryption, and 1 through 132 characters with encryption.
The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

---

ecs

Permits the user to use ACS-specific configuration commands. Default: Permitted

---

expiry-date *date_time*

Specifies the date and time that this login account expires.
Enter the date and time in the YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss format. Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

---

ftp

Permits the user to use FTP and SFTP. Default: Not permitted

li-administration

Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

nocli

Prevents the user from using the command line interface. Default: Permitted

noecs

Prevents the user from accessing ACS-specific commands.

timeout-absolute *timeout_absolute*

Important: This keyword is obsolete. It has been left in place for backward compatibility. If used, a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum time, in seconds, the Security Administrator may have a session active before the session is forcibly terminated. *timeout_absolute* must be an integer from 0 through 300000000.
The value 0 disables this timeout configuration.
Default: 0

timeout-min-absolute *timeout_min_absolute*

Specifies the maximum time (in minutes) the Security Administrator may have a session active before the session is forcibly terminated. *timeout_min_absolute* must be an integer from 0 through 525600. The value 0 disables this timeout configuration. Default: 0

timeout-idle *timeout_idle*

Important: This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum time, in seconds, the Security Administrator may have a session active before the session is terminated. *timeout_idle* must be an integer from 0 through 300000000.
The value 0 disables the idle timeout configuration.
Default: 0

timeout-min-idle *timeout_min_idle*

Specifies the maximum time, in minutes, the Security Administrator may have a session active before the session is terminated. *timeout_min_idle* must be an integer from 0 through 525600. The value 0 disables the idle timeout configuration. Default: 0

Usage

Use this command to create new Security Administrators or modify existing user's settings.
Security Administrator users have read-write privileges and full access to all contexts and command modes.
Refer to the *Command Line Interface Overview* chapter for more information.

Important: A maximum of 128 administrative users and/or subscribers may be locally configured per context.

Example

The following command creates a Security Administrator account named *user1* with access to ACS configuration commands:

```
administrator user1 password secretPassword
```

The following removes the Security Administrator account named *user1*:

```
no administrator user1
```

apn

Creates or deletes Access Point Name (APN) templates and enters the APN Configuration Mode within the current context.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

[no] apn *apn_name* **[-noconfirm]**

no

Deletes a previously configured APN template.

apn_name

Specifies a name for the APN template as an alphanumeric string of 1 through 62 characters that is case insensitive. It may also contain dots (.) and/or dashes (-).

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

WARNING: If this keyword option is used with the **no apn** *apn_name* command, the APN named *apn_name* will be deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage

This command creates an APN within the system and causes the CLI to enter the APN Configuration Mode. The APN is a logical name for a packet data network and/or a service to which the system supports access. When a create PDP context request is received by the system, it examines the APN information element within the packet. The system determines if an APN with the identical name is configured. If so, the system uses the configuration parameters associated with that APN as a template for processing the request. If the names do not match, the request is rejected with a cause code of 219 (DBH, Missing or unknown APN). APN templates should be created/configured within destination contexts on the system. Up to 1000 APNs can be configured.

Example

The following command creates an APN template called *isp1*:

```
apn isp1
```

asn-qos-descriptor

Creates, deletes or manages the Quality of Service (QoS) descriptor table identifier for Access Service Node Gateway (ASN-GW) service and enters the ASN QoS Descriptor Table Identifier Configuration mode within the source context.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

asn-qos-descriptor id *qos_table_id* **[default] dscp [be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af 42 | af 43 | ef] [-noconfirm]**

no asn-qos-descriptor *qos_table_id* **[default] dscp [be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af 42 | af 43 | ef] [-noconfirm]**

no

Deletes a preciously configured ASN QoS descriptor table identifier.

asn-qos-descriptor id *qos_table_id*

Specifies a unique identifier for ASN QoS descriptor table to create/configure. *qos_table_id* must be an integer from 1 through 65535.

[default] dscp

Specifies DSCP marking for this QoS descriptor.

[be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af 42 | af 43 | ef]

The DSCP marking for this QoS descriptor. Default value is be (best effort).

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

WARNING: If this keyword option is used with **no asn-qos-descriptor id** *qos_table_id* command the ASN QoS descriptor table with identifier *qos_table_id* will be deleted with all active/inactive configurations without prompting any warning or confirmation.

Usage

Use this command to configure a QoS description table to manage QoS functionality for an ASN-GW service subscriber. This command creates and allows the configuration of QoS tables with in a context. This command is also used to remove previously configured ASN-GW services QoS descriptor table.
A maximum of 16 QoS Descriptor Tables can be configured per system.
Refer to the *ASN QoS Descriptor Configuration Mode Commands* chapter of this reference for additional information.

Example

The following command creates a QoS descriptor table with identifier *1234* for the ASN-GW service subscribers:

```
asn-qos-descriptor id 1234
```

asn-service-profile

Creates, deletes or manages the Service Profiles Identifier for Access Service Node Gateway (ASN-GW) service subscribers and enters the ASN Service Profile Configuration mode within the current context.

Product

ASN-GW

Privilege

Administrator

Syntax

asn-service-profile id *asn_profile_id* **direction { bi-directional | downlink | uplink } [activation-trigger {activate | admit | dynamic-reservation | provisioned } [-noconfirm]**

no asn-service-profile id *asn_profile_id* **[-noconfirm]**

no

Deletes a preciously configured ASN service profile identifier.

asn-service-profile id *asn-profile_id*

Specifies a unique identifier for ASN profile to create/configure.

direction { bi-directional | downlink | uplink }

Specifies the direction of data traffic to apply this service profile.
bi-directional: Enables this service profile in both direction of uplink and downlink.
downlink: Enables this service profile in downlink direction, towards the subscriber.
uplink: Enables this service profile in uplink direction, towards the system.

activation-trigger {activate | admit | dynamic-reservation | provisioned

Use this option to configure the activation-trigger for the asn-service-profile. Default: provisioned | admit | activate

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

WARNING: If this keyword option is used with **no asn-service-profile id** *asn_profile_id* command the ASN service profile with identifier *asn_profile_id* will be deleted with all active/inactive configurations without prompting any warning or confirmation.

Usage

Use this command to configure a service profile to apply the ASN-GW service subscribers. This command creates and allows the configuration of service profiles with in a context. This command is also used to remove previously configured ASN-GW services profiles.
A maximum of 32 ASN Service Profiles can be configured per context.

Refer to the *ASN Service Profile Configuration Mode Commands* chapter of this reference for additional information.

Example

The following command creates an ASN Service Profile with identifier *1234* for the ASN-GW service subscribers:

```
asn-service-profile id 1234 direction uplink
```

asngw-service

Creates, deletes or manages an Access Service Node Gateway (ASN-GW) service and enters the ASN Gateway Service Configuration Mode within the current context.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

asngw-service *asngw_name* **[-noconfirm]**

no asn-service *asngw_name* **[-noconfirm]**

no

Deletes a previously configured ASN-GW service.

asngw-service *asngw_name*

Specifies the name of the ASN-GW service to create/configure as an alphanumeric string of 1 through 63 characters that is case sensitive.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

WARNING: If this keyword option is used with **no asn-service** *asngw_name* command the ASN-GW service named *asngw_name* will be deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage

Services are configured within a context and enable certain functionality. This command creates and allows the configuration of services enabling the system to function as an ASN Gateway in a WiMAX network. This command is also used to remove previously configured ASN-GW services.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Refer to the *ASN Gateway Service Configuration Mode Commands* chapter of this reference for additional information.

Example

The following command creates an ASN-GW service name *asn-gw1*:

```
asngw-service asn-gw1
```

asnpc-service

Creates, deletes or manages an ASN Paging Controller service to manage the ASN paging controller service and enters the ASN Paging Controller Configuration mode within the current context.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

[no] asnpc-service *asn_pc_svc_name* **[-noconfirm]**

no

Deletes a preciously configured ASN paging controller service.

asnpc-service *asn_pc_svc_name*

Specifies the name of the ASN Paging Controller Service to create and enable as an alphanumeric string of 1 through 63 characters that is case sensitive.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

WARNING: If this keyword option is used with **no asnpc-service** *asn_pc_svc_name* command the ASN Paging Controller service named *asn_pc_svc_name* will be deleted and disabled with all active/inactive paging groups and paging agents configured in a context for ASN paging controller service without prompting any warning or confirmation.

Usage

Use this command to create and enable the ASN paging controller services in the system to provide functionality of an ASN Paging Controller service within a context. Additionally this command provides the access to the ASN Paging Controller Service Configuration mode and also used to remove previously configured ASN Paging Controller services.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Refer to the *ASN Paging Controller Service Configuration Mode Commands* chapter of this reference for additional information.

Example

The following command creates an ASN paging controller service name *asnpc_1*:

```
asnpc-service asnpc_1
```

bfd-protocol

Enables or disables Bidirectional Forwarding Detection (BFD) protocol and enters the BFD Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] bfd-protocol
```

Usage

Use this command to set configuration parameters for detecting faults in paths established with BFD-enabled routers.
Refer to the *BFD Configuration Mode Commands* chapter for additional information.

Example

The following command enables BFD Configuration mode:

```
bfd-protocol
```

bgp extended-asn-cap

Enables or disables the router to send 4-octet ASN capabilities.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] bgp extended-asn-cap
```

Example

The following command enables the router to send 4-octet ASN Capabilities:

```
bgp extended-asn-cap
```

bmsc-profile

Creates or deletes Broadcast Multicast Service Center (BM-SC) profiles and enters the BMSC Profile Configuration Mode within the current context.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

[no] bmsc-profile name *bmsc_profile_name* [**-noconfirm**]

no

Deletes a previously configured BM-SC profile.

bmsc-profile name *bmsc_profile_name*

Specifies a name for the BM-SC profile as an alphanumeric string of 1 through 62 characters that is case insensitive. It may also contain dots (.) and/or dashes (-).

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

WARNING: If this keyword option is used with **no bmsc-profile name** *bmsc_profile_name* command the BM-SC profile named *bmsc_profile_name* is deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage

Use this command to create a BM-SC profile within the context and take the user to enter the BMSC Profile Configuration Mode.
The BM-SC profile is a logical name for a Broadcast Multicast Service Center in Multimedia Broadcast and Multicast service.
BM-SC profile should be created/configured within contexts on the system. Up to four BM-SC profiles can be configured.

Example

The following command creates a BM-SC Profile called *mbms_sc_1*:

```
bmsc-profile name mbms_sc_1
```

busyout ip pool

Makes addresses from an IP pool in the current context unavailable once they are free.

Product

PDSN, HA, GGSN, NAT

Privilege

Security Administrator, Administrator

Syntax

busyout ip pool { all | all-dynamic | all-static | name *pool_name* **} [address-range** *start_address end_address* **| lower-percentage** *percent* **| upper-percentage** *percent* **]**

no busyout ip pool { all | all-dynamic | all-static | name *pool_name* **} [address-range** *start_address end_address* **| lower-percentage** *percent* **| upper-percentage** *percent* **]**

no

Disables the busyout command specified.

busyout ip pool all

Applies to all IP pools in the current context.

busyout ip pool all-dynamic

Applies to all dynamic IP-pools in the current context.

busyout ip pool all-static

Applies to all static IP pools in the current context.

busyout ip pool name *pool_name*

Applies the named IP pool or IP pool group in the current context. *pool_name* must be the name of an existing IP pool or IP pool group in the current context.

address-range *start_address end_address*

Busyout all addresses from *start_address* through *end_address*. *start_address*: The beginning IP address of the range of addresses to busyout. This IP address must exist in the pool specified and entered in IPv4 dotted-decimal notation.
end_address: The ending IP address of the range of addresses to busyout. This IP address must exist in the pool specified and entered in IPv4 dotted-decimal notation.

lower-percentage *percent*

Busyout the percentage of IP addresses specified, beginning at the lowest numbered IP address. This is a percentage of all of the IP addresses in the specified IP pool. *percent* must be an integer from 0 through 100.

upper-percentage *percent*

Busyout the percentage of IP addresses specified, beginning at the highest numbered IP address. This is a percentage of all of the IP addresses in the specified IP pool. *percent* must be an integer from 0 through 100.

Usage

Use this command to busyout IP addresses when resizing an IP pool.
Up to 32 instances of this command can be executed per context.
A single instance of this command can busy-out multiple IP address pools in the context through the use of the **all**, **all-static**, or **all-dynamic** keywords.

Example

Assume an IP pool named *Pool10* with addresses from *192.168.100.1* through *192.168.100.254*. To busy out the addresses from *192.168.100.50* through *192.169.100.100*, enter the following command:

```
busyout ip pool name Pool10 address-range 92.168.100.50 192.169.100.100
```

To restore the IP addresses from the previous example and make them accessible again, enter the following command:

```
no busyout ip pool name Pool10 address-range 92.168.100.50
192.169.100.100
```

cae-group

Creates a CAE group, which is a CAE server cluster that services TCP video requests from the Mobile Video Gateway. The Mobile Video Gateway uses the configured CAE group for CAE load balancing. The CAE (Content Adaptation Engine) is an optional component of the Mobile Videoscape.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

[no] cae-group *cae_group_name* **[-noconfirm]**

---

no cae-group *cae_group_name*

Deletes the CAE group if previously configured.

---

cae-group *cae_group_name*

Creates the specified CAE group and enters the Video Group Configuration Mode. *cae_group_name* is an alphanumeric string of 1 through 79 characters.

-noconfirm

Executes the command without any prompt and confirmation from the user.

Usage

Use this command to create a CAE group and enter the Video Group Configuration Mode. This command gets issued from the Context Configuration Mode.

Example

The following command creates a CAE group named *group_1* and enters the Video Group Configuration Mode:

```
cae-group group_!
```

camel-service

Creates an instance of the Customized Applications for Mobile Enhanced Logic (CAMEL) service and enters the CAMEL service configuration mode. This mode configures or edits the configuration for the parameters which control the CAMEL functionality on the SGSN.

Important: For details about the commands and parameters, check the *CAMEL Service Configuration Mode* chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

camel-service *srvc_name*

no camel-service *srvc_name*

no

Remove the configuration for the specified SGSN service from the configuration of the current context.

camel-service *srvc_name*

Creates a CAMEL service instance having a unique name expressed as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to create, edit, or remove an CAMEL service

Example

The following command creates an CAMEL service named *camel1* in the current context:

```
camel-service camel1
```

The following command removes the CAMEL service named *camel2* from the configuration for the current context:

```
no camel-service camel2
```

cipher-suite

Creates a new SSL cipher suite or specifies an existing cipher suite and enters the Cipher Suite Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

`[ no ] cipher-suite` *`name`*

`no`

Removes the specified SSL cipher suite from the context.

`cipher-suite` *`name`*

Specifies the name of a new or existing SSL cipher suite as n alphanumeric string of 1 through 127 characters that must be unique across all CSCF services within the same context and across all contexts.

Usage

Use this command to create a new SSL cipher suite or modify an existing one.

Important: One SSL cipher suite can be created per SSL template.

A cipher suite contains the cryptographic algorithms supported by the client, and defines a key exchange and a cipher spec, which specifies the encryption and hash algorithms used during authentication. SSL cipher suites allow operators to select levels of security and to enable communication between devices with different security requirements.
Entering this command results in the following prompt:

```
[context_name]hostname(cfg-ctx-cipher-suite)#
```

Cipher Suite Configuration Mode commands are defined in the *Cipher Suite Configuration Mode Commands* chapter.

Example

The following command specifies the SSL cipher suite *`cipher_suite_1`* and enters the Cipher Suite Configuration Mode:

```
cipher-suite cipher_suite_1
```

class-map

Creates or deletes a class map. If the class-map is newly created, the system enters the Class-Map Configuration Mode within the current destination context to configure the match rules for packet classification to flow-based traffic policing for a subscriber session flow.

Product

PDSN, HA, ASN-GW, HSGW

Privilege

Security Administrator, Administrator

Syntax

`[ no ] class-map name` *`class_name`* **`[ match-all | match-any ]`**

`no`

Deletes configured Class-Map within the context.

`lass-map name` *`class_name`*

Specifies the name of Class-Map rule as an alphanumeric string of 1 through 15 characters and is case sensitive.

`match-all`

Default: Enabled.
Enables AND logic for all matching parameters configured in specific Class-Map to classify traffic flow/packets. It indicates to match all classification rules in specific Class-Map to consider the specified Class-Map as a match.

`match-any`

Default: Disabled.
Enables OR logic for matching parameters configured in specific Class-Map to classify traffic flow/packets. It indicates to match any of the classification rule in specific Class-Map to consider the specified Class-Map as a match.

Usage

Use this command to enter in Class-Map Configuration Mode to set classification parameters or filters in traffic policy for a subscriber session flow.

Important: In this mode classification rules added sequentially with **match** command to form a Class-Map. To change and/or delete or re-add a particular rule entire Class-Map is required to delete.

Example

Following command configures classification map *`class_map1`* with option to match any condition in match rule.

```
class-map name class_map1 match-any
```

closedrp-rp handoff

Enables or disables session handoff between Closed-RP and RP connections. Default: Disabled

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
closedrp-rp handoff

[ default | no ] closedrp-rp handoff
```

default

Resets the command to its default setting of disabled.

no

Disables Closed-RP to RP session handoff.

closedrp-rp handoff

Enables Closed-RP to RP session handoff.

Usage

Use this command to enable a PDSN service to handoff sessions between Closed-RP and RP connections.

Example

To enable Closed-RP to RP handoffs, use the following command:

```
closedrp-rp handoff
```

To disable Closed-RP to RP handoffs, use the following command:

```
no closedrp-rp handoff
```

config-administrator

Configures a context-level administrator account within the current context.

Product

All

Privilege

Security Administrator

Syntax

config-administrator *user_name* **[encrypted] password** *password* **[ecs] [expiry-date** *date_time* **] [ftp] [li-administration] [nocli] [noecs] [timeout-absolute** *abs_seconds* **] [timeout-min-absolute** *abs_minutes* **] [timeout-idle** *timeout_duration* **] [timeout-min-idle** *idle_minutes* **]**

no config-administrator *user_name*

no

Removes a previously configured context-level administrator account.

config-administrator *user_name*

Specifies the name for the account as an alphanumeric string of 1 through 32 characters.

[encrypted] password *password*

Specifies the password to use for the user which is being given context-level administrator privileges within the current context. The encrypted keyword indicates the password specified uses encryption.
password is an alphanumeric string of 1 through 63 characters without encryption, or 1 through 127 characters with encryption.
The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

ecs

Permits the user access to ACS-specific configuration commands. Default: Enhanced Charging Service (ECS / ACS) specific configuration commands allowed.

expiry-date *date_time*

Specifies the date and time that this account expires in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.
Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

ftp

Indicates the user gains FTP and SFTP access with the administrator privileges. Default: FTP and SFTP are not allowed.

li-administration

Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

nocli

Indicates the user is not allowed to access the command line interface. Default: CLI access allowed.

noecs

Prevents the specific user from accessing ACS-specific configuration commands.

timeout-absolute *abs_seconds*

Important: This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum amount of time (in seconds) that the administrator may have a session active before the session is forcibly terminated. *abs_seconds* must be an integer from 0 through 300000000. The value 0 disables the absolute timeout. Default: 0

timeout-min-absolute *abs_minutes*

Specifies the maximum amount of time (in minutes) the context-level administrator may have a session active before the session is forcibly terminated. *abs_minutes* must be an integer from 0 through 525600 (365 days). The value 0 disables the absolute timeout. Default: 0

timeout-idle *timeout_duration*

Important: This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum amount of idle time, in seconds, the context-level administrator may have a session active before the session is terminated. *timeout_duration* must be a value in the range from 0 through 300000000. The value 0 disables the idle timeout. Default: 0

timeout-min-idle *idle_minutes*

Specifies the maximum amount of idle time, in minutes, the context-level administrator may have a session active before the session is terminated. *idle_minutes* must be a value in the range from 0 through 525600 (365 days). The value 0 disables the idle timeout. Default: 0

Usage

Create new context-level administrators or modify existing administrator's options, in particular, the timeout values.
Administrator users have read-write privileges and full access to all contexts and command modes (except for a few security functions). Refer to the *Command Line Interface Overview* chapter of this guide for more information.

Important: A maximum of 128 administrative users and/or subscribers may be locally configured per context.

Example

The following configures a context-level administration named *user1* with ACS parameter control:

```
config-administrator user1 password secretPassword ecs
```

The following command removes a context-level administrator named *user1*:

```
no config-administrator user1
```

content-filtering

Enables or disables the creation, configuration or deletion of Content Filtering Server Groups (CFSG).

Product

CF

Privilege

Security Administrator, Administrator

Syntax

content-filtering server-group *cf_server_group_name* **[-noconfirm]**

no content-filtering server-group *cf_server_group_name*

no

Removes the specified CFSG previously configured in this context.

content-filtering server-group *cf_server_group_name*

Specifies the name of the CFSG as an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any prompt and confirmation from the user.

Usage

Use this command to create/configure/delete a CFSG.

Example

The following command creates a CFSG named *CF_Server1*:

```
content-filtering server-group CF_Server1
```

credit-control-service

Enables or disables the creation, configuration or deletion of credit-control services.

Product

All

Privilege

Security Administrator, Administrator

Syntax

credit-control-service *service_name* **[-noconfirm]**

no credit-control-service *service_name*

no

Deletes the specified credit-control service.

credit-control-service *service_name*

Specifies name of the credit-control service as an alphanumeric string of 1 through 63 characters.
If the named credit-control service does not exist, it is created, and the CLI mode changes to the Credit Control Service Configuration Mode wherein the service can be configured.
If the named credit-control service already exists, the CLI mode changes to the Credit Control Service Configuration Mode wherein the service can be configured.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to create, configure or delete credit-control services.
Entering this command results in the following prompt:
`[context_name]hostname(config-credit-control-service)`
Credit control service configuration commands are described in the *Credit Control Service Configuration Mode Commands* chapter.

Example

The following command enters the Credit Control Service Configuration Mode for a credit-control service named *test159*:

```
credit-control-service test159
```

crypto group

Creates or deletes a crypto group and enters the Crypto Configuration Mode allowing the configuration of crypto group parameters.

Product

PDSN, PDIF, HA, GGSN

Privilege

Administrator, Config-Administrator

Syntax

[no] crypto group *group_name*

no

Deletes a previously configured crypto group.

[no] crypto group *group_name*

Specifies the name of the crypto group as an alphanumeric string of 1 through 127 characters that is case sensitive.

Important: A maximum of 32 crypto groups per context can be configured.

Usage

Use this command to enter the configuration mode allowing the configuration of crypto group parameters. Crypto (tunnel) groups are used to support the Redundant IPSec Tunnel Fail-over feature and consist of two configured ISAKMP crypto maps. Each crypto map defines the IPSec policy for a tunnel. In the crypto group, one tunnel serves as the primary, the other as the secondary (redundant).

Example

The following command configures a crypto group called *group1*:

```
crypto group group1
```

crypto ipsec transform-set

Configures transform-sets on the system and enters the Crypto Trans Configuration Mode.

Product

PDSN, PDIF, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
crypto ipsec transform-set transform_name [ ah { hmac { md5-96 | none | sha1-96 } { esp {
hmac { { md5-96 | sha1-96 } { cipher { 3des-cbc | aes-cbc-128 | aes-cbc-256 | des-cbc } }
| none } } } } ]

no crypto ipsec transform-set transform_name
```

no

Removes a previously configured transform set

crypto ipsec transform-set *transform_name*

Specifies the name of the transform set as an alphanumeric string of 1 through 127 characters that is case sensitive.

ah hmac

Configures the Authentication Header (AH) hash message authentication codes (HMAC) parameter for the transform set to one of the following:

- **md5-96**: Message Digest 5 truncated to 96 bits
- **none**: Disables the use of the AH protocol for the transform set.
- **sha1-96**: Secure Hash Algorithm-1 truncated to 96 bits

esp hmac

Configures the Encapsulating Security Payload (ESP) hash message authentication codes (HMAC) parameter for the transform set to one of the following:

- **md5-96**: Message Digest 5 truncated to 96 bits
- **none**: Disables the use of the AH protocol for the transform set.
- **sha1-96**: Secure Hash Algorithm-1 truncated to 96 bits

cipher

If ESP is enabled, this option must be used to set the encapsulation cipher protocol to one of the following:

- **3des-cbc**: Triple Data Encryption Standard (3DES) in chain block (CBC) mode.
- **aes-cbc-128**: Advanced Encryption Standard (AES) in CBC mode with a 128-bit key.
- **aes-cbc-256**: Advanced Encryption Standard (AES) in CBC mode with a 256-bit key.
- **des-cbc**: DES in CBC mode.

Usage

Use this command to create a transform set on the system.
Transform Sets are used to define IPSec security associations (SAs). IPSec SAs specify the IPSec protocols to use to protect packets.
Transform sets are used during Phase 2 of IPSec establishment. In this phase, the system and a peer security gateway negotiate one or more transform sets (IPSec SAs) containing the rules for protecting packets. This negotiation ensures that both peers can properly protect and process the packets.

Important: The **ah** and subsequent keywords are required when the transform set is initially configured.

Example

Create a transform set that has the name *tset1*, no authentication header, an encapsulating security protocol header hash message authentication code of **md5**, and a bulk payload encryption algorithm of **des-cbc** with the following command:

```
crypto ipsec transform-set tset1 ah hmac none esp hmac md5 cipher des-cbc
```

crypto map

Configures the name of the policy and enters the specified Crypto Map Configuration mode.

Product

PDSN, HA, GGSN, P-GW, PDIF

Privilege

Security Administrator, Administrator

Syntax

```
crypto map name [ ikev2-ipv6 | ipsec-dynamic | ipsec-ikev1 | ipsec-manual ]

no crypto map name
```

no

Removes a previously configured crypto map.

crypto map *name*

Specifies the name of the crypto map as an alphanumeric string of 1 through 127 characters that is case sensitive.

ikev2-ipv6

Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

ipsec-dynamic

Creates a dynamic crypto map and/or enters the Crypto Map Dynamic Configuration Mode.

ipsec-ikev1

Creates an IKEv1 crypto map and/or enters the Crypto Map IKEv1 Configuration Mode.

ipsec-manual

Creates a manual crypto map and/or enters the Crypto Map Manual Configuration Mode.

Usage

Crypto Maps define the policies that determine how IPSec is implemented for subscriber data packets. There are several types of crypto maps supported by the system. They are:

- **Manual crypto maps**: These are static tunnels that use pre-configured information (including security keys) for establishment. Because they rely on statically configured information, once created, the tunnels never expire; they exist until their configuration is deleted.

Important: Because manual crypto map configurations require the use of static security keys (associations), they are not as secure as crypto maps that rely on dynamically configured keys. Therefore, it is recommended that they only be configured and used for testing purposes.

- **IKEv1 crypto maps**: These tunnels are similar to manual crypto maps in that they require some statically configured information such as the IP address of a peer security gateway and that they are applied to specific system interfaces. However, IKEv1 crypto maps offer greater security because they rely on dynamically generated security associations through the use of the Internet Key Exchange (IKE) protocol.
- **IKEv2-IPv6 crypto maps**: Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.
- **Dynamic crypto maps:** These tunnels are used for protecting L2TP-encapsulated data between the system and an LNS/security gateway or Mobile IP data between an FA service configured on one system and an HA service configured on another.

Important: The crypto map type (dynamic, IKEv1, IKEv2-IPv6, or manual) is specified when the map is first created using this command.

Example

Create a dynamic crypto map named *map1* and enter the Crypto Map Dynamic Configuration Mode by entering the following command:

```
crypto map map1 ipsec-dynamic
```

crypto template

Creates a new or specifies an existing crypto template and enters the Crypto Template Configuration Mode.

Product

PDIF, S-GW

Privilege

Security Administrator, Administrator

Syntax

crypto template *name* **ikev2-dynamic**

no crypto template *name*

no

Deletes a previously configured crypto template.

crypto template *name* **ikev2-pdif**

Specifies the name of a new or existing crypto template as an alphanumeric string of 1 through 127 characters.

ikev2-dynamic

Configures the Crypto Template to be used for configuring IPSec functionality.

Usage

Use this command to create a new or enter an existing crypto template.
Entering this command results in the following prompt:

```
[context_name]hostname(cfg-crypto-tmpl-ikev2-tunnel)#
```

Crypto Template Configuration Mode commands are defined in the *Crypto Template Configuration Mode Commands* chapter.

Example

The following command configures a IKEv2 dynamic crypto template called *crypto1* and enters the Crypto Template Configuration Mode:

```
crypto template crypto1 ikev2-dynamic
```

cscf access-profile

Creates a new or enters an existing access profile used to set signaling compression for various network access types.

Product

SCM

Privilege

Administrator

Syntax

cscf access-profile { default | name *profile_name* **} [-noconfirm]**

no cscf access-profile name *profile_name*

default

Specifies that the system is to enter the Access Profile Configuration Mode for the default access profile.

cscf access-profile name *profile_name*

Specifies a name for the access profile as an alphanumeric string of 1 through 79 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no cscf access-profile name *profile_name*

Removes the CSCF access profile from the context.

Usage

Use this command to create an access profile for the CSCF service and cause the system to enter the Access Profile Configuration Mode where parameters are configured for the profile.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-access-profile)#
```

Access Profile Configuration Mode commands are defined in the *CSCF Access Profile Configuration Mode Commands* chapter.

Example

The following command creates a CSCF Access Profile named *profile2* and enters the Access Profile Configuration Mode:

```
cscf access-profile name profile2
```

cscf acl

Creates an Access Control List (ACL) and enters the ACL Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

cscf acl { default | name *list_name* **} [-noconfirm]**

no cscf acl name *list_name*

default

Specifies that the system is to enter the ACL Configuration Mode for the default ACL.

cscf acl name *list_name*

Specifies a name for the ACL as an alphanumeric string of 1 through 47 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no cscf acl name *list_name*

Removes the CSCF ACL from the context.

Usage

Use this command to create an access control list for the CSCF service and cause the system to enter the ACL Configuration Mode where parameters are configured for the new list.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-acl)#
```

ACL Configuration Mode commands are defined in the *CSCF ACL Configuration Mode Commands* chapter.
Use this command when configuring the following SCM components: P-CSCF, S-CSCF, and SIP Proxy.

Example

The following command creates a CSCF access control list named *acl1* and enters the ACL Configuration Mode:

```
cscf acl name acl1
```

cscf diameter-selection

Creates a CDF or HSS diameter selection table and enters the CSCF Diameter Selection Configuration Mode.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
cscf diameter-selection type { cdf | hss } [ -noconfirm ]

no cscf diameter-selection type { cdf | hss }
```

type { cdf | hss }

Specifies the type of diameter selection table.
cdf: Diameter selection table for selecting CDF server
hss: Diameter selection table for selecting HSS server

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no cscf diameter-selection type { cdf | hss }

Removes the specified CDF or HSS diameter selection table.

Usage

Use this command to cause the system to enter the Diameter Selection Configuration Mode where parameters are configured for the diameter group.

Important: When HSS table has entries, this criteria is always applied for HSS server selection. CDF server selection, however, can be enabled or disabled for a given access type.

Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-diameter-selection)#
```

Diameter Selection Configuration Mode commands are defined in the *CSCF Diameter Selection Configuration Mode Commands* chapter.
Use this command when configuring the S-CSCF.

Example

The following command creates an HSS diameter selection table and enters the Diameter Selection Configuration Mode:

```
cscf diameter-selection type hss
```

cscf ifc-filter-criteria

Creates Initial Filter Criteria (iFC) filter criteria for shared iFC functionality.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

cscf ifc-filter-criteria id *fc_id* **priority** *pri* **[profile-part-indicator { registered | unregistered }] app-server uri scheme { sip | sips }** *as* **as-default-handling { session-continue | session-terminate } [-noconfirm] | [service-info** *info* **] [trigger-point** *tp_name* **] [-noconfirm] | [trigger-point** *tp_id* **] [-noconfirm]**

no cscf ifc-filter-criteria id *fc_id*

cscf ifc-filter-criteria id *fc_id*

Specifies an ID for the iFC filter criteria as an integer from 1 through 200.

priority *pri*

Specifies the priority of the filter criteria, which is used to select a particular filter criteria from multiple ones present under an ISC template. *pri* must be an integer from 0 through 1024.

profile-part-indicator { registered | unregistered }

Indicates whether the iFC is a part of the **registered** or **unregistered** user profile. If a value is not specified, then the configuration will be applied to both registered and unregistered subscribers.

app-server uri scheme { sip | sips }

Determines the associated application server's URI scheme.
sip: SIP URI
sips: SIPS URI (TLS)

as

Specifies an address for the associated application server as an alphanumeric string of 1 through 127 characters.

as-default-handling { session-continue | session-terminate }

Determines whether the dialog should be released (**session-terminate**) or not (**session-continue**) when the application server could not be reached or on application server error is returned.

-noconfirm

Executes command without any additional prompt and confirmation from the user.

service-info *info*

Specifies optional service information to be sent to the application server. *info* is an alphanumeric string of 1 trough 63 characters.

trigger-point *tp_id*

Assigns an iFC trigger point to the filter criteria as an integer from 1 through 200.

no cscf ifc-filter-criteria id *fc_id*

Removes the specified CSCF iFC filter criteria from the context.

Usage

Use this command to create a filter criteria ID and associate an application server address to it. You may also define a trigger point ID to be executed in order to select the application server. If no trigger point is specified, then the application server is selected unconditionally.

Important: Filter criteria is associated with an ISC template in the ISC Template Configuration Mode.

Important: Filter criteria can be assigned to more than one ISC template.

Example

The following command creates a iFC filter criteria *15*, which has a priority of 2 and is part of the registered user profile. Filter criteria *15* is assigned to a sip application server named *appserver*. The dialog will not be released if the application server can not be reached. Filter criteria *15* is also assigned trigger point *12*:

```
cscf ifc-filter-criteria id 15 priority 2 profile-part-indicator
registered app-server uri scheme sip appserver as-default-handling
session-continue trigger-point 12
```

cscf ifc-spt-condition

Creates an Initial Filter Criteria (iFC) Service Point Trigger (SPT) condition for shared iFC functionality.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

cscf ifc-spt-condition id *cond_id* **{ request-uri content** *uri_content* **| session-case { originating-registered | originating-unregistered | terminating-registered | terminating-unregistered } | session-description** *sdp* **[content** *sdp_data* **] | sip-header** *hdr* **[content** *hdr_data* **] | sip-method** *method* **} [-noconfirm] [condition-negated]**

no cscf ifc-spt-condition id *cond_id*

cscf ifc-spt-condition id *cond_id*

Specifies an ID for the iFC SPT condition as an integer from 1 through 200.

request-uri content *uri_content*

Specifies request URI content as an alphanumeric string of 1 through 127 characters.

Important: Wildcard Extended Regular Expressions (ERE) are supported for this value. For example, "sip.user[0-9]@192\\.168\\.176\\.150"

session-case { originating-registered | originating-unregistered | terminating-registered | terminating-unregistered }

Determines the type of session:

- **originating-registered**: Session handling an originating end user.
- **originating-unregistered**: Session handling an unregistered originating end user.
- **terminating-registered**: Session handling a terminating registered end user.
- **terminating-unregistered**: Session handling a terminating unregistered end user.

session-description *sdp* **[content** *sdp_data* **]**

Specifies an SDP line type.
sdp is an alphanumeric string of 1 through 15 characters.
content specifies content on the SDP line.
sdp_data is an alphanumeric string of 1 through 127 characters.

sip-header *hdr* **[content** *hdr_data* **]**

Specifies a header type.
hdr is an alphanumeric string of 1 through 127 characters.
content specifies content on the header.
hdr_data is an alphanumeric string of 1 through 127 characters.

sip-method *method*

Specifies a sip method.
method is an alphanumeric string of 1 through 127 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

condition-negated

Negates the specified condition.

no cscf ifc-spt-condition id *cond_id*

Removes the specified CSCF iFC SPT condition from the context.

Usage

Use this command to create individual SPT conditions that are later associated with an SPT group in the iFC SPT Group Configuration Mode.

Important: An iFC SPT group may be associated with multiple SPT conditions.

Example

The following command creates iFC SPT condition *10* which handles an originating end user:

```
cscf ifc-spt-condition id 10 session-case originating-registered
```

The following command negates the condition created above:

```
cscf ifc-spt-condition id 10 session-case originating-registered
condition-negated
```

cscf ifc-spt-group

Creates an Initial Filter Criteria (iFC) Service Point Trigger (SPT) group for shared iFC functionality.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

cscf ifc-spt-group id *group_id* **[[-noconfirm] | reg-type { de-registration | initial-registration | re-registration } [-noconfirm]]**

no cscf ifc-spt-group id *group_id*

cscf ifc-spt-group id *group_id*

Specifies an ID for the iFC SPT group as an integer from 1 through 200.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

reg-type { de-registration| initial-registration | re-registration }

Defines whether the SPT condition matches to REGISTER messages that are related to:

- **de-registration**
- **initial-registration**
- **re-registration**

no cscf ifc-spt-group id *group_id*

Removes the specified CSCF iFC SPT group from the context.

Usage

Use this command to create an iFC SPT group ID and bind different SPT conditions under it.

Important: An iFC SPT group may be associated with multiple SPT conditions.

The SPT group can also specify the registration type that defines whether the SPT condition matches to REGISTER messages that are related to initial registrations, re-registrations, or de-registrations.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-ifc-spt-group)#
```

iFC SPT Group Configuration Mode commands are defined in the *CSCF IFC SPT Group Configuration Mode Commands* chapter.

Example

The following command creates iFC SPT group *21*:

```
cscf ifc-spt-group id 21
```

cscf ifc-trigger-point

Creates an Initial Filter Criteria (iFC) trigger point for shared iFC functionality.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

cscf ifc-trigger-point id *tp_id* **condition-type { cnf | dnf } [-noconfirm]**

no cscf ifc-trigger-point id *tp_id*

cscf ifc-trigger-point id *tp_id*

Specifies an ID for the iFC trigger point as an integer from 1 through 200.

condition-type { cnf | dnf }

Defines the condition type of the iFC trigger point:
cnf: conjunctive normal form
dnf: disjunctive normal form

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no cscf ifc-trigger-point id *tp_id*

Removes the specified CSCF iFC trigger point from the context.

Usage

Use this command to create a trigger point ID and bind different SPT groups under it.

Important: An iFC SPT group can be assigned to more than one iFC trigger point.

Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-ifc-trigger-point)#
```

IFC Trigger Point Configuration Mode commands are defined in the *CSCF IFC Trigger Point Configuration Mode Commands* chapter.

Example

The following command creates iFC trigger point *11* with a **cnf** condition type:

```
cscf ifc-trigger-point id 11 condition-type cnf
```

cscf isc-template

Creates an IMS Service Control (ISC) template and enters the ISC Template Configuration Mode.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

[no] cscf isc-template id *template_id*

no

Removes the CSCF ISC template from the context.

cscf isc-template id *template_id*

Specifies an ID for the ISC template as an integer from 1 through 200.

Usage

Use this command to create an ISC template for the CSCF service and cause the system to enter the ISC Template Configuration Mode where parameters are configured for the new template.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-isc-tmpl)#
```

ISC Template Configuration Mode commands are defined in the *CSCF ISC Template Configuration Mode Commands* chapter.
Use this command when configuring the following SCM component: S-CSCF.

Example

The following command creates ISC template *10* and enters the ISC Template Configuration Mode:

```
cscf isc-template id 10
```

cscf last-route-profile

Creates a last route profile, which will be specified on peer server configuration to select the Last Routing Option (LRO) number while forwarding an emergency call packet to a particular peering server, and enters the Last Route Profile Criteria Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

cscf last-route-profile name *profile_name* **criteria { county-name | round-robin } [-noconfirm]**

no cscf last-route-profile name *profile_name*

---

cscf last-route-profile name *profile_name*

Specifies the name of the last route profile as an alphanumeric string of 1 through 79 characters.

---

criteria { county-name | round-robin }

county-name: Profile specific to the county-name criteria.
Entering this command results in the following prompt:

```
[context_name]hostname(config-county-name-lro-profile)#
```

Last Route Profile Criteria Configuration Mode commands are defined in the *CSCF Last Route Profile Criteria Configuration Mode Commands* chapter.
round-robin: Profile specific to the round-robin criteria.
Entering this command results in the following prompt:

```
[context_name]hostname(config-round-robin-lro-profile)#
```

Last Route Profile Criteria Configuration Mode commands are defined in the *CSCF Last Route Profile Criteria Configuration Mode Commands* chapter.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

---

no cscf last-route-profile name *profile*

Removes the specified CSCF last route profile from the context.

Usage

Use this command to create a last route profile and enter the Last Route Profile Criteria Configuration Mode.

Important: Last route profiles are associated with peer servers in the CSCF Peer Server Monitoring Configuration Mode.

Use this command when configuring the following SCM components: S-CSCF and SIP Proxy.

Example

The following command creates a last route profile named *lro1* and enters the CSCF Last Route Profile Criteria Configuration Mode to specify county name criteria:

```
cscf last-route-profile name lro1 criteria county-name
```

The following command creates a last route profile named *lro2* and enters the CSCF Last Route Profile Criteria Configuration Mode to specify round robin criteria:

```
cscf last-route-profile name lro2 criteria round-robin
```

cscf peer-servers

Creates a peer server type for next-hop session routing and enters the Peer Servers Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

cscf peer-servers *server_name* **type { type } [-noconfirm]**

no cscf peer-servers *server_name*

cscf peer-servers *server_name*

Specifies the name of the peer server as an alphanumeric string of 1 through 79 characters.

type { type }

Specifies the type of peer server to configure:

- **bgcf**: Border Gateway Control Function
- **ecscf**: Emergency Call/Session Control Function
- **ibcf**: Interconnect Border Control Function
- **icscf**: Interrogating Call/Session Control Function
- **mgcf**: Media Gateway Control Function
- **mrfc**: Media Resource Function Controller
- **other**: Other Function
- **pcscf**: Proxy Call/Session Control Function
- **scscf**: Serving Call/Session Control Function
- **sip-as**: Session Initiation Protocol-Application Server

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no cscf peer-servers *server_name*

Removes the specified CSCF peer server from the context.

Usage

Use this command to create a specific peer server and enter the Peer Servers Configuration Mode where connectivity parameters can be entered.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-peer-servers)#
```

Peer Servers Configuration Mode commands are defined in the *CSCF Peer Servers Configuration Mode Commands* chapter.
Use this command when configuring the following SCM components: E-CSCF, P-CSCF, S-CSCF, and SIP Proxy.

Example

The following command creates an I-CSCF server type called *icscf_peer1* and enters the Peer Servers Configuration Mode:

```
cscf peer-servers icscf_peer1 type icscf
```

cscf peer-servers-group

Creates a peer servers group and enters the Peer Servers Group Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

cscf peer-servers-group *group_name* **type sip-as [-noconfirm]**

no cscf peer-servers-group *group_name*

cscf peer-servers-group *group_name*

Specifies the name of the peer servers group as an alphanumeric string of 1 through 79 characters.

type sip-as

Specifies that the type of peer servers group to configure is **sip-as** (Session Initiation Protocol-Application Server).

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no cscf peer-servers-group *group_name*

Removes the specified CSCF peer servers group from the context.

Usage

Use this command to create a specific peer servers group and enter the Peer Servers Group Configuration Mode where peer servers lists can be managed.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-peer-servers-group)#
```

Peer Servers Group Configuration Mode commands are defined in the *CSCF Peer Servers Group Configuration Mode Commands* chapter.

Example

The following command creates a peer servers group called *group1* and enters the Peer Servers Group Configuration Mode:

```
cscf peer-servers-group group1 type sip-as
```

cscf policy

Creates a policy group for specific AoR profiles and enters the Policy Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

cscf policy { default | name *policy_name* **[-noconfirm] }**

no cscf policy name *policy_name*

---

default

Specifies that the system is to enter the AoR Policy Rules Configuration Mode for the default policy. The default policy uses AoR policy rules.
Entering this command results in the following prompt:
[*context_name*]*hostname*(config-aor-policy)#
Default (AoR) Policy Configuration Mode commands are defined in the *CSCF AoR Policy Rules Configuration Mode Commands* chapter.

---

cscf policy name *policy_name*

Specifies the name of the policy group as an alphanumeric string of 1 through 79 characters.
Entering this command results in the following prompt:
[*context_name*]*hostname*(config-cscf-policy)#
Policy Configuration Mode commands are defined in the *CSCF Policy Configuration Mode Commands* chapter.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

---

no cscf policy name *policy_name*

Removes the specified CSCF policy group from the context.

Usage

Use this command to create a policy group and enter either the AoR Policy Rules Configuration Mode (**default**) or Policy Configuration Mode (**name** *policy_name*).
Use this command when configuring the following SCM components: P-CSCF, S-CSCF, and SIP Proxy.

Example

The following command creates a policy group named *group2* and enters the CSCF Policy Configuration Mode:

```
cscf policy name group2
```

cscf prefix-table

Creates a CSCF prefix table and enters the CSCF Prefix Table Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

```
[ no ] cscf prefix-table
```

no

Removes the prefix table.

Usage

Use this command to create a CSCF prefix table and cause the system to enter the Prefix Table Configuration Mode. The prefix table is used to configure for each number (or number prefix) whether it is ported and the SIP routing domain.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-prefix-table)#
```

Prefix Table Configuration Mode commands are defined in the *CSCF Prefix Table Configuration Mode Commands* chapter.

Example

The following command creates a CSCF prefix table and enters the Prefix Table Configuration Mode:

```
cscf prefix-table
```

cscf routes

Creates a route group for specifying routing information and enters the Routes Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

cscf routes { default | name *route_name* **[-noconfirm] }**

no cscf routes name *route_name*

---

default

Specifies that the system is to enter the Routes Configuration Mode for the default route group.

---

cscf routes name *route_name*

Specifies the name of the route group as an alphanumeric string of 1 through 79 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

---

no cscf routes name *route_name*

Removes the specified CSCF route group from the context.

Usage

Use this command to create a route group and enter the Routes Configuration Mode.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-route)#
```

Routes Configuration Mode commands are defined in the *CSCF Routes Configuration Mode Commands* chapter.
Use this command when configuring the following SCM components: P-CSCF, S-CSCF, SIP Proxy.

Example

The following command creates a route group named *route_group5* and enters the Route Group Configuration Mode:

```
cscf routes name route_group5
```

cscf service

Creates a CSCF service or specifies an existing CSCF service and enters the CSCF Service Configuration Mode for the current context.

Product

SCM

Privilege

Administrator

Syntax

cscf service *service_name* **[-noconfirm]**

no cscf service *service_name*

cscf service *service_name*

Specifies the name of the CSCF service. If *service_name* does not refer to an existing service, the new service is created if resources allow.
service_name is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no cscf service *service_name*

Removes the specified CSCF service from the context.

Usage

Enter the CSCF Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-service)#
```

CSCF Service Configuration Mode commands are defined in the *CSCF Service Configuration Mode Commands* chapter.
Use this command when configuring the following SCM components: P-CSCF, S-CSCF, SIP Proxy.

Example

The following command enters the existing CSCF Service Configuration Mode (or creates it if it does not already exist) for the service named *cscf-service1*:

```
cscf service cscf-service1
```

The following command will remove *cscf-service1* from the system:

```
no cscf service cscf-service1
```

cscf session-template

Creates a session template and/or enters the Session Template Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

cscf session-template { default | name *template_name* **[-noconfirm] }**

no cscf session-template name *template_name*

default

Specifies that the system is to enter the Session Template Configuration Mode for the default session template.

cscf session-template name *template_name*

Specifies a name for the template as an alphanumeric string of 1 through 79 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no cscf session-template name *template_name*

Removes the specified CSCF session template from the context.

Usage

Use this command to create a new session template and enter the Session Template Configuration Mode or enter the mode for an existing template.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-session-template)#
```

Session Template Configuration Mode commands are defined in the *CSCF Session Template Configuration Mode Commands* chapter.
Use this command when configuring the following SCM components: P-CSCF, S-CSCF, SIP Proxy.

Example

The following command enters the Session Template Configuration Mode for a template named *sess_temp4*:

```
cscf session-template name sess_temp4
```

cscf subdomain-routes

Creates subdomain-route list and enters the Subdomain-route List Configuration Mode.

Product

SCM (I-CSCF)

Privilege

Administrator

Syntax

`[ no ] cscf subdomain-routes`

`no`

Removes the CSCF subdomain-route list from the context.

`cscf subdomain-routes`

Creates the CSCF subdomain-route list within the context.

Usage

Use this command to create a subdomain-route list and enter the Subdomain-route List Configuration Mode. I-CSCF, upon receiving the terminating request, checks the subdomain-route list for matches. If a match is found, the routing will happen based on it. Otherwise, I-CSCF performs a User Location Query (Location-Information-Request) before proceeding.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-subdomain-route)#
```

Subdomain-route List Configuration Mode commands are defined in the *CSCF Subdomain-route List Configuration Mode Commands* chapter.

Example

The following command enters the Subdomain-route List Configuration Mode:

```
cscf subdomain-routes
```

cscf translation

Creates a translation list and enters the Translation Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

cscf translation { default | name *list_name* **[-noconfirm] }**

no cscf translation name *list_name*

default

Specifies that the system is to enter the Translation Configuration Mode for the default translation list.

cscf translation name *list_name*

Specifies a name for the translation list as an alphanumeric string of 1 through 79 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no cscf translation name *list_name*

Removes the specified CSCF translation list from the context.

Usage

Use this command to create a new translation list and enter the Translation Configuration Mode or enter the mode for an existing list.
Translation lists are used to modify or replace a request-URI such as an E.164 number. For example, a translation list can be configured to append digits to the end of a number or replace a domain name with another.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-translation)#
```

Translation Configuration Mode commands are defined in the *CSCF Translation Configuration Mode Commands* chapter.
Use this command when configuring the following SCM components: P-CSCF, S-CSCF, SIP Proxy.

Example

The following command enters the Translation Configuration Mode for a translation list named *trans_list3*:

```
cscf translation name trans_list3
```

cscf urn-service-list

Creates a URN service list and enters the URN List Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

cscf urn-service-list { default | name *list_name* **[-noconfirm] }**

no cscf urn-service-list name *list_name*

default

Specifies that the system is to enter the URN List Configuration Mode for the default URN service list.

cscf urn-service-list name *list_name*

Specifies a name for the URN service list as an alphanumeric string of 1 through 79 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no cscf urn-service-list name *list_name*

Removes the specified CSCF URN service list from the context.

Usage

Use this command to create a URN service list name and enter the URN List Configuration Mode. URN lists contain URN to URI mappings used for emergency and location-based services. A URN service list is selected by a CSCF session template.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-service-urn)#
```

URN List Configuration Mode commands are defined in the *CSCF URN List Configuration Mode Commands* chapter.
Use this command when configuring the following SCM components: P-CSCF.

Example

The following command enters the URN List Configuration Mode for a URN list named *urn_list1*:

```
cscf urn-service-list name urn_list1
```

css server

This is a restricted command. In Release 9.0 and later, this command is obsolete.

dhcp-service

Adds a Dynamic Host Control Protocol (DHCP) service instance to the current context and enters the configuration mode for that service.

Product

GGSN, ASN-GW, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

dhcp-service *service_name* **[no] allow dhcp-relay-agent-auth-suboption[-noconfirm]**

no dhcp-service *service_name*

no

Removes a previously configured DHCP service from the current context.

dhcp-service *service_name*

Specifies the name of the DHCP service as an alphanumeric string of 1 through 63 characters that is case sensitive.

allow dhcp-relay-agent-auth-suboption

The DHCP Relay Agent Information Option conveys information between a DHCP Relay Agent and a DHCP server. This specification defines an authentication suboption for that option, containing a keyed hash in its payload. The suboption supports data integrity and replay protection for relayed DHCP messages.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

WARNING: If this keyword option is used with **no dhcp-service** *service_name* command the DHCP service named *service_name* is deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage

Use this command to add a DHCP service to a context configured on the system and enter the DHCP Service Configuration Mode. A DHCP service is a logical grouping of external DHCP servers.
The DHCP Configuration Mode provides parameters that dictate the system's communication with one or more of these DHCP servers.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Refer to the *DHCP Service Configuration Mode* chapter of this reference for additional information.

Example

The following command creates a DHCP service called *dhcp1* and enter the DHCP Service Configuration Mode:

```
dhcp-service dhcp1
```

diameter accounting

This command configures Diameter accounting related settings.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter accounting { dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | nasreq | rf-plus } | endpoint *endpoint_name* **| hd-mode fall-back-to-local | hd-storage-policy** *hd_policy* **| max-retries** *max_retries* **| max-transmissions** *transmissions* **| request-timeout** *duration* **| server** *host_name* **priority** *priority* **}**

default diameter accounting { dictionary | hd-mode | max-retries | max-transmissions | request-timeout }

no diameter accounting { endpoint | hd-mode | hd-storage-policy | max-retries | max-transmissions | server *host_name* **}**

---

no diameter accounting { endpoint | hd-mode | hd-storage-policy | max-retries | max-transmissions | server *host_name* **}**

endpoint: Removes the currently configured accounting endpoint. The default accounting server configured in the default AAA group will be used.
hd-mode: Sends records to the Diameter server, if all Diameter servers are down or unreachable, then copies records to the local HDD and periodically retries the Diameter server.
hd-storage-policy: Disables use of the specified HD storage policy.
max-retries: Disables the retry attempts for Diameter accounting in this AAA group.
max-transmissions: Disables the maximum number of transmission attempts for Diameter accounting in this AAA group.
server *host_name*: Removes the Diameter host *host_name* from this AAA server group for Diameter accounting.

---

default diameter accounting { dictionary | hd-mode | max-retries | max-transmissions | request-timeout }

dictionary: Sets the context's dictionary to the default.
hd-mode: Sends records to the Diameter server, if all Diameter servers are down or unreachable, then copies records to the local HDD and periodically retries the Diameter server.
max-retries: 0 (disabled)
max-transmissions: 0 (disabled)
request-timeout: 20 seconds

---

dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | nasreq | rf-plus }

Specifies the Diameter accounting dictionary.

aaa-custom1 ... aaa-custom10: Configures the custom dictionaries. Even though the CLI syntax supports several custom dictionaries, not necessarily all of them have been defined. If a custom dictionary that has not been implemented is selected, the default dictionary will be used.
nasreq: nasreq dictionary—the dictionary defined by RFC 3588.
rf-plus: RF Plus dictionary.

---

endpoint *endpoint_name*

Enables Diameter to be used for accounting, and specifies which Diameter endpoint to use.
endpoint_name is an alphanumeric string of 1 through 63 characters.

---

hd-mode fall-back-to-local

Specifies that records be copied to the local HDD if the Diameter server is down or unreachable. CDF/CGF will pull the records through SFTP.

---

hd-storage-policy *hd_policy*

Specifies the HD Storage policy name.
hd_policy must be the name of a configured HD Storage policy, expressed as an alphanumeric string of 1 through 63 characters.
HD storage policies are configured through the Global Configuration Mode.
This and the **hd-mode** command are used to enable the storage of Rf Diameter Messages to HDD in case all Diameter Servers are down or unreachable.

---

max-retries *max_retries*

Specifies how many times a Diameter request should be retried with the same server, if the server fails to respond to a request.
max_retries specifies the maximum number of retry attempts. The value must be an integer from 1 through 1000.
Default: 0

---

max-transmissions *transmissions*

Specifies the maximum number of transmission attempts for a Diameter request. Use this in conjunction with the "**max-retries** *max_retries*" option to control how many servers will be attempted to communicate with.
transmissions specifies the maximum number of transmission attempts for a Diameter request. The value must be an integer from 1 through 1000. Default: 0

---

request-timeout *duration*

Specifies how long the system will wait for a response from a Diameter server before re-transmitting the request.
duration specifies the number of seconds the system will wait for a response from a Diameter server before re-transmitting the request. This value must be an integer from 1 through 3600. Default: 20

---

server *host_name* **priority** *priority*

Specifies the current context Diameter accounting server's host name and priority.
host_name specifies the Diameter host name, expressed as an alphanumeric string of 1 through 63 characters.
priority specifies the relative priority of this Diameter host. The priority is used in server selection. The priority must be an integer from 1 through 1000.

Usage

Use this command to manage the Diameter accounting options according to the Diameter server used for the context.

Example

The following command configures the Diameter accounting dictionary as **aaa-custom4**:

```
diameter accounting dictionary aaa-custom4
```

The following command configures the Diameter endpoint named *aaaa_test*:

```
diameter accounting endpoint aaaa_test
```

diameter authentication

This command configures Diameter authentication related settings.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter authentication { dictionary { aaa-custom1 | aaa-custom10 | aaa-custom11 | aaa-custom12 | aaa-custom13 | aaa-custom14 | aaa-custom15 | aaa-custom16 | aaa-custom17 | aaa-custom18 | aaa-custom19 | aaa-custom2 | aaa-custom20 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | nasreq } | endpoint *endpoint_name* **| max-retries** *max_retries* **| max-transmissions** *transmissions* **| redirect-host-avp { just-primary | primary-then-secondary } | request-timeout** *duration* **| server** *host_name* **priority** *priority* **}**

default diameter authentication { dictionary | max-retries | max-transmissions | redirect-host-avp | request-timeout }

no diameter authentication { endpoint | max-retries | max-transmissions | server *host_name* **}**

---

no diameter authentication { endpoint | max-retries | max-transmissions | server *host_name* **}**

- **endpoint**: Removes the authentication endpoint. The default server configured in default AAA group will be used.
- **max-retries**: Disables the retry attempts for Diameter authentication in this AAA group.
- **max-transmissions**: Disables the maximum transmission attempts for Diameter authentication in this AAA group.
- **server** *host_name*: Removes the Diameter host *host_name* from this AAA server group for Diameter authentication.

---

default diameter authentication { dictionary | max-retries | max-transmissions | redirect-host-avp | request-timeout }

Configures default setting for specified parameter.

- **dictionary**: Sets the context's dictionary to the default.
- **max-retries**: Sets the retry attempts for Diameter authentication requests in this AAA group to default 0 (disable).
- **max-transmissions**: Sets the configured maximum transmission attempts for Diameter authentication in this AAA group to default 0 (disable).
- **redirect-host-avp**: Sets the redirect choice to default (just-primary).
- **request-timeout**: Sets the timeout duration, in seconds, for Diameter authentication requests in this AAA group to default (20).

dictionary { aaa-custom1 | aaa-custom10 | aaa-custom11 | aaa-custom12 | aaa-custom13 | aaa-custom14 | aaa-custom15 | aaa-custom16 | aaa-custom17 | aaa-custom18 | aaa-custom19 | aaa-custom2 | aaa-custom20 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | nasreq }

Specifies the Diameter authentication dictionary.
aaa-custom1 ... aaa-custom8, aaa-custom10 ... aaa-custom20: Configures the custom dictionaries. Even though the CLI syntax supports several custom dictionaries, not necessarily all of them have been defined. If a custom dictionary that has not been implemented is selected, the default dictionary will be used.

Important: **aaa-custom11** dictionary is only available in Release 8.1 and later. **aaa-custom12** to **aaa-custom20** dictionaries are only available in Release 9.0 and later releases.

aaa-custom9: Configures the STa standard dictionary.
nasreq: nasreq dictionary—the dictionary defined by RFC 3588.

endpoint *endpoint_name*

Enables Diameter to be used for authentication, and specifies which Diameter endpoint to use.
endpoint_name is an alphanumeric string of 1 through 63 characters.

max-retries *max_retries*

Specifies how many times a Diameter authentication request should be retried with the same server, if the server fails to respond to a request.
max_retries specifies the maximum number of retry attempts, and must be an integer from 1 through 1000. Default: 0

max-transmissions *transmissions*

Specifies the maximum number of transmission attempts for a Diameter authentication request. Use this in conjunction with the "**max-retries** *max_retries*" option to control how many servers will be attempted to communicate with.
transmissions specifies the maximum number of transmission attempts, and must be an integer from 1 through 1000. Default: 0

diameter authentication redirect-host-avp { just-primary | primary-then-secondary }

Specifies whether to use just one returned AVP, or use the first returned AVP as selecting the primary host and the second returned AVP as selecting the secondary host.
just-primary: Redirect only to primary host.
primary-then-secondary: Redirect to primary host, if fails then redirect to the secondary host.
Default: **just-primary**

request-timeout *duration*

Specifies how long the system will wait for a response from a Diameter server before re-transmitting the request.
duration specifies the number of seconds the system will wait for a response from a Diameter server before re-transmitting the request, and must be an integer from 1 through 3600. Default: 20

server *host_name* **priority** *priority*

Specifies the current context Diameter authentication server's host name and priority.
host_name specifies the Diameter host name, expressed as an alphanumeric string of 1 through 63 characters.
priority specifies the relative priority of this Diameter host, and must be an integer from 1 through 1000. The priority is used in server selection.

Usage

Use this command to manage the Diameter authentication configurations according to the Diameter server used for the context.

Example

The following command configures the Diameter authentication dictionary *aaa-custom14*:

```
diameter authentication dictionary aaa-custom14
```

The following command configures the Diameter endpoint named *aaau1*:

```
diameter authentication endpoint aaau1
```

diameter authentication failure-handling

This command configures error handling for Diameter EAP requests.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } { request-timeout action { continue | retry-and-terminate | terminate } | result-code *result_code* **{ [to** *end_result_code* **] action { continue | retry-and-terminate | terminate } } }**

no diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } result-code *result_code* **[to** *end_result_code* **]**

default diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } request-timeout action

---

no

Disables Diameter authentication failure handling.

---

default

Configures the default Diameter authentication failure handling setting.

---

authorization-request

Specifies that failure handling is to be performed on Diameter authorization request messages (AAR/AAA).

---

eap-request

Specifies configuring failure handling for EAP requests.

---

eap-termination-request

Specifies configuring failure handling for EAP termination requests.

---

request-timeout action { continue | retry-and-terminate | terminate }

Specifies the action to be taken for failures:

- **continue**: Continues the session
- **retry-and-terminate**: First retries, if it fails then terminates the session
- **terminate**: Terminates the session

---

result-code *result_code* **{ [to** *end_result_code* **] action { continue | retry-and-terminate | terminate } }**

result_code: Specifies the result code, must be an integer from 1 through 65535.

to *end_result_code*: Specifies the upper limit of a range of result codes. *end_result_code* must be greater than *result_code*.
action { continue | retry-and-terminate | terminate }: Specifies action to be taken for failures:

- **continue**: Continues the session
- **retry-and-terminate**: First retries, if it fails then terminates the session
- **terminate**: Terminates the session

Usage

Use this command to configure error handling for Diameter EAP, EAP-termination, and authorization requests. Specific actions (continue, retry-and-terminate, or terminate) can be associated with each possible result-code. Ranges of result codes can be defined with the same action, or actions can be specific on a per-result code basis.

Example

The following commands configure result codes 5001, 5002, 5004, and 5005 to use **action continue** and result code 5003 to use a**ction terminate**:

```
diameter authentication failure-handling eap-request result-code 5002 to
5005 action continue

diameter authentication failure-handling eap-request result-code 5003
action terminate
```

diameter dictionary

This command is deprecated and is replaced by the **diameter accounting dictionary** and **diameter authentication dictionary** commands. See **diameter accounting** and **diameter authentication** commands respectively.

diameter endpoint

This command enables the creation, configuration or deletion of a Diameter endpoint.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter endpoint *endpoint_name* **[-noconfirm]**

no diameter endpoint *endpoint_name*

no

Removes the specified Diameter endpoint.

endpoint_name

Specifies name of the Diameter endpoint as an alphanumeric string of 1 through 63 characters that should be unique within the system.
If the named endpoint does not exist, it is created, and the CLI mode changes to the Diameter Endpoint Configuration Mode wherein the endpoint can be configured.
If the named endpoint already exists, the CLI mode changes to the Diameter Endpoint Configuration Mode wherein the endpoint can be reconfigured.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to create/configure/delete a Diameter origin endpoint.
Entering this command results in the following prompt:
`[context_name]hostname(config-ctx-diameter)`
Diameter origin endpoint configuration commands are described in the *Diameter Endpoint Configuration Mode Commands* chapter.

Example

The following command changes to the Diameter Endpoint Configuration CLI mode for Diameter origin endpoint named *test13*:

```
diameter endpoint test13
```

diameter sctp

This command configures Diameter SCTP parameters for all Diameter endpoints within the context. In 12.2 and later releases, this command is obsolete and replaced with **associate sctp-parameter-template**command in Diameter Endpoint Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter sctp { hearbeat-interval *interval* **| path max-retransmissions** *retransmissions* **}**

default diameter sctp { heartbeat-interval | path max-retransmissions }

default

Configures this command with the default settings.

- **heartbeat-interval**: Sets the heartbeat interval to the default value.
- **path max-retransmissions**: Sets the SCTP path maximum retransmissions to the default value.

hearbeat-interval *interval*

Specifies the time interval between heartbeat chunks sent to a destination transport address in seconds.
interval must be an integer from 1 through 255.
Default: 30 seconds

path max-retransmissions *retransmissions*

Specifies the maximum number of consecutive retransmissions over a destination transport address of a peer endpoint before it is marked as inactive.
retransmissions must be an integer from 1 through 10.
Default: 10

Usage

Use this command to configure Diameter SCTP parameters for all diameter endpoints within the context.

Example

The following command configures the heartbeat interval to *60* seconds:

```
diameter sctp hearbeat-interval 60
```

The following command configures the maximum number of consecutive retransmissions to *6*, after which the endpoint is marked as inactive:

```
diameter sctp path max-retransmissions 6
```

diameter origin

This command is deprecated and is replaced by the **diameter endpoint** command.

dns-client

Creates a DNS client and/or enters the DNS Client Configuration Mode.

Product

SCM, SGSN, MME, P-GW

Privilege

Security Administrator, Administrator

Syntax

[no] dns-client *name* **[-noconfirm]**

no

Removes the specified DNS client from the context.

dns-client *name*

Specifies a name for the DNS client as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to create a new DNS client and enter the DNS Client Configuration Mode or enter the mode for an existing client.
Entering this command results in the following prompt:

```
[context_name]hostname(config-dns-client)#
```

DNS Client Configuration Mode commands are defined in the *DNS Client Configuration Mode Commands* chapter.

Example

The following command enters the DNS Client Configuration Mode for a DNS client named *dns1*:

```
dns-client dns1
```

domain

Configures a domain alias for the current context.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

domain [*] *domain_name* **[default subscriber** *subs_temp_name* **]**

no domain [*] *domain_name*

no domain [*] *domain_name*

Indicates the domain specified is to be removed as an alias to the current context.

domain [*] *domain_name*

domain_name specifies the domain alias to create/remove from the current context. If the domain portion of a subscribers user name matches this value, the current context is used for that subscriber.
domain_name is an alphanumeric string of 1 through 79 characters. The domain name can contain all special characters, however note that the character * (wildcard character) is only allowed at the beginning of the domain name.
If the domain name is prefixed with * (wildcard character), and an exact match is not found for the domain portion of a subscriber's user name, subdomains of the domain name are matched. For example, if the domain portion of a subscriber's user name is abc.xyz.com and you use the domain command **domain** **xyz.com* it matches. But if you do not use the wildcard (**domain** *xyz.com*) it does not match.

Important: The domain alias specified must not conflict with the name of any existing context or domain names.

default subscriber *subs_temp_name*

Specifies the name of the subscriber template to apply to subscribers using this domain alias.
subs_temp_name is an alphanumeric string of 1 through 127 characters. If this keyword is not specified the default subscriber configuration in the current context is used.

Usage

Set a domain alias when a single context may be used to support multiple domains via aliasing.

Example

```
domain sampleDomain.net

no domain sampleDomain.net
```

eap-profile

Creates a new, or specifies an existing, Extensible Authentication Protocol (EAP) profile and enters the EAP Configuration Mode.

Product

ASN-GW, PDIF

Privilege

Security Administrator, Administrator

Syntax

[no] eap-profile *name*

eap-profile *name*

Specifies the name of a new or existing EAP profile as an alphanumeric string of 1 through 256 characters.

Usage

Use this command to create a new or enter an existing EAP profile.
Entering this command results in the following prompt:

```
[context_name]hostname(config-ctx-eap-profile)#
```

EAP Configuration Mode commands are defined in the *EAP Configuration Mode Commands* chapter.

Example

The following command configures an EAP profile called *eap1* and enters the EAP Configuration Mode:

```
eap-profile eap1
```

edr-module active-charging-service

Enables the creation, configuration or deletion of the Event Data Record (EDR) module for this context.

Product

ACS, GGSN, HA, LNS, PDSN, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] edr-module active-charging-service [ charging | reporting ]
```

no

Removes the EDR module configuration for the current context.

edr-module active-charging-service

Enables the EDR data module for this context.

charging

Enables the EDR module for charging EDRs that are stored in the /records/edr directory.

reporting

Enables the EDR module for reporting EDRs that are stored in the /records/redr directory.

Usage

Use this command to create the EDR module for the context, and configure the EDR module for active charging service records. You must be in a non-local context when specifying this command, and you must use the same context when specifying the UDR module command.
If this CLI command is configured without the **charging** or **reporting** keywords, by default the EDR module is enabled for charging EDRs.

Example

The following command creates the EDR module for the context for charging EDRs, and enters the EDR Module Configuration Mode:

```
edr-module active-charging-service
```

egtp-service

Creates an eGTP service or specifies an existing eGTP service and enters the eGTP Service Configuration Mode for the current context.

Product

MME, P-GW, S-GW

Privilege

Administrator

Syntax

egtp-service *service_name* **[-noconfirm]**

no egtp-service *service_name*

egtp-service *service_name*

Specifies the name of the eGTP service as an alphanumeric string of 1 through 63 characters. If *service_name* does not refer to an existing service, the new service is created if resources allow.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no egtp-service *service_name*

Removes the specified eGTP service from the context.

Usage

Enter the eGTP Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-egtp-service)#
```

eGTP Service Configuration Mode commands are defined in the *eGTP Service Configuration Mode Commands* chapter.
Use this command when configuring the following GTP SAE components: MME, P-GW, and S-GW.

Example

The following command enters the existing eGTP Service Configuration Mode (or creates it if it does not already exist) for the service named *egtp-service1*:

```
egtp-service egtp-service1
```

The following command will remove *egtp-service1* from the system:

```
no egtp-service egtp-service1
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

event-notif-endpoint

Enables creation, configuration or deletion of an Event Notification collection server endpoint.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

[no] event-notif-endpoint *en_node_name*

no

Removes the specified Event Notification collection server endpoint.

event-notif-endpoint *en_node_name*

Specifies name of the Event Notification collection server endpoint as an alphanumeric string of 1 through 31 characters.
If the named endpoint does not exist, it is created, and the CLI mode changes to the Event Notification Interface Endpoint Configuration Mode wherein the endpoint can be configured.
If the named endpoint already exists, the CLI mode changes to the Event Notification Interface Endpoint Configuration Mode wherein the endpoint can be reconfigured.

Usage

Use this command to create/configure/delete an Event Notification collection server endpoint.
Only 1 Event Notification interface across a chassis can be configured on a system.
Entering this command results in the following prompt:

```
[context_name]hostname(config-ntfyintf-endpoint)#
```

The commands configured in this mode are defined in the *Event Notification Interface Endpoint Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Caution: This is a critical configuration. The PCC Event notification can not be collected on a server without this configuration. Any change to this configuration would lead to the loss of event notifications from PCC service on IPCF node.

Example

The following command creates an Event Notification Interface Endpoint named *event_intfc_3*:

```
event-notif-endpoint event_intfc_3
```

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

external-inline-server

This is a restricted command.

fa-service

Creates or deletes a foreign agent (FA) service or specifies an existing FA service for which to enter the FA Service Configuration Mode for the current context.

Product

PDSN, ASN-GW, FA

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] fa-service name
```

no

Indicates the foreign agent service specified is to be removed.

fa-service *name*

Specifies the name of the FA service to configure as an alphanumeric string of 1 through 63 characters. If *name* does not refer to an existing service, the new service is created if resources allow.

Usage

Enter the FA Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

The following command will enter the FA Service Configuration Mode creating the service *sampleService*, if necessary.

```
fa-service sampleService
```

The following command will remove *sampleService* as being a defined FA service.

```
no fa-service sampleService
```

firewall max-associations

This command is obsolete.

fng-service

Creates a new, or specifies an existing FNG service and enters the FNG Service Configuration Mode. A maximum of 16 FNG services can be created. This limit applies per ASR 5000 chassis and per context.

Product

FNG

Privilege

Security Administrator, Administrator

Syntax

fng-service *name* **[-noconfirm]**

no fng-service *name*

fng-service *name*

Specifies the name of a new or existing FNG service as an alphanumeric string of 1 through 63 characters that must be unique across all FNG services within the same context and across all contexts.

no fng-service *name*

Deletes the specified FNG service.

Usage

Use this command in Context Configuration Mode to create a new FNG service or modify an existing one. Executing this command enters the FNG Service Configuration Mode.

Example

The following command configures an FNG service named *fng1* and enters the FNG Service Configuration Mode:

```
fng-service fmg1
```

ggsn-service

Creates or deletes a Gateway GPRS Support Node (GGSN) service and enters the GGSN Service Configuration Mode within the current context to configure it.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

ggsn-service *svc_name* **[-noconfirm]**

no ggsn-service *svc_name*

no

Deletes a preciously configured GGSN service.

ggsn-service *svc_name*

Specifies the name of the GGSN service to create/configure as an alphanumeric string of 1 through 63 characters that is case sensitive.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Services are configured within a context and enable certain functionality. This command creates and allows the configuration of services enabling the system to function as a GGSN in a GPRS or UMTS network. This command is also used to remove previously configured GGSN services.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

The following command creates a GGSN service named *ggsn1*:

```
ggsn-service ggsn1
```

gprs-service

Creates a GPRS service instance and enters the GPRS Service Configuration Mode. This mode configures all of the parameters specific to the operation of an SGSN in a GPRS network.

Important: For details about the commands and parameters for this mode, check the *GPRS Service Configuration Mode* chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gprs-service *srvc_name*

no gprs-service *srvc_name*

no

Removes the configuration for the specified IGPRS service from the configuration for the current context.

gprs-service *srvc_name*

Specifies the name of the GPRS service as a unique alphanumeric string of 1 through 63 characters.

Usage

Use this command to create or remove a GPRS service. Entering this command will move the system to the GPRS Service Configuration Mode and change the prompt to:

```
[context_name]hostname(config-gprs-service)#
```

Example

The following command creates an GPRS service named *gprs1*:

```
gprs-service gprs1
```

The following command removes the GPRS service named *gprs1*:

```
no gprs-service gprs1
```

gs-service

Creates a Gs service instance and enters the Gs Service Configuration Mode. This mode configures the parameters specific to the Gs interface between the SGSN and the MSC/VLR.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gs-service *svc_name* **[-noconfirm]**

no gs-service *svc_name*

no

Remove the configured Gs service from the current context.

gs-service *svc_name*

Specifies the Gs service as a unique alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to create, edit, or remove a Gs service.
A maximum of 32 Gs service can be configured in one context/system. This limit is subject to maximum of 256 services (regardless of type) can be configured per system.

Important: For details about the commands and parameters for this mode, refer *Gs Service Configuration Mode* chapter.

Example

The following command creates an Gs service named *gs1*:

```
gs-service gs1
```

The following command removes the Gs service named *gs1*:

```
no gs-service gs1
```

gtpp algorithm

Configures GTPP routing algorithms for the current context.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

gtpp algorithm { first-server | round-robin | first-n *count* **}**

gtpp algorithm first-server

Specifies that accounting data is sent to the first available charging gateway function (CGF) based upon the relative priority of each configured CGF. Default: Enabled

gtpp algorithm round-robin

Specifies that accounting data is transmitted in a circular queue fashion such that data is sent to the highest priority CGF first, then to the next available CGF of the highest priority, and so on. Ultimately, the queue returns to the CGF with the highest configured priority. Default: Disabled

gtpp algorithm first-n *count*

Specifies that the AGW must send accounting data to *count* (more than one) CGFs based on their priority. Response from any one of the *count* CGFs would suffice to proceed with the call. The full set of accounting data is sent to each of the *count* CGFs.
count is the number of CGFs to which accounting data will be sent, and must be an integer from 2 through 65535. Default: 1 (Disabled)

Usage

Use this command to control how G-CDR/P-CDR accounting data is routed among the configured CGFs.

Example

The following command configures the system to use the round-robin algorithm when transmitting G-CDR/P-CDR accounting data:

```
gtpp algorithm round-robin
```

gtpp attribute

Allows the specification of the optional attributes to be present in the call detail records (CDRs) that the GPRS/PDN/UMTS access gateway generates. It also defines that how the information is presented in CDRs by encoding the attribute field values.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp attribute { apn-ni | apn-selection-mode | charging-characteristic-selection-mode | cell-plmn-id | diagnostics | duration-ms | dynamic flag | imei | local-record-sequence-number | losdv | ms-timezone | msisdn | |node-id | | node-id-suffix *suffix* **| pdn-connection-id | pdp-address | pdp-type | pgw-plm-id | plmn-id [unknown-use** *uncode_value* **] | rat | record-extensions rat | served-mnai | served-pdp-pdn-address-extension | sms { destination-number | recording-entity | service-centre } | start time | stop time | uli }**

default gtpp attribute { apn-ni | apn-selection-mode | charging-characteristic-selection-mode | cell-plmn-id | diagnostics | duration-ms | dynamic flag | imei | local-record-sequence-number | losdv | ms-timezone | msisdn | node-id | pdn-connection-id | pdp-address | pdp-type | pgw-plm-id | plmn-id | rat | record-extensions | served-mnai | served-pdp-pdn-address-extension | sms { destination-number | recording-entity | service-centre } | start time | stop time | uli }

no gtpp attribute { apn-ni | apn-selection-mode | charging-characteristic-selection-mode | cell-plmn-id | diagnostics | duration-ms | dynamic flag | imei | local-record-sequence-number | losdv | ms-timezone | msisdn | node-id | node-id-suffix | pdn-connection-id | pdp-address | pdp-type | pgw-plm-id | plmn-id | rat | record-extensions | served-mnai | served-pdp-pdn-address-extension | sms { destination-number | recording-entity | service-centre } | start time | stop time | uli }

default

Sets the default GTPP attributes in generated the CDRs. It also sets the default presentation of attribute values in generated CDRs.

no

Removes the configured GTPP attributes from the CDRs.

apn-ni

Default: Enabled
Includes the APN field in the CDR that is created.
This keyword is applicable for P-GW and GGSN only.

apn-selection-mode

Default: Enabled

Includes the APN Selection Mode field in the CDR that is created.
This keyword is applicable for P-GW and GGSN only.

charging-characteristics-selection-mode

Default: Enabled
Includes the Charging Characteristic Selection Mode field in the CDR that is created.
This keyword is applicable for P-GW and GGSN only.

cell-plmn-id

Default: Disabled
This keyword configures the SGSN to include the cell's PLMN identifier (MCC and MNC) in generated CDRs (M-CDRs and/or the S-CDRs).
This keyword is applicable for SGSN only.

diagnostics

Default: Disabled
Includes the Diagnostic field in the CDR that is created when PDP contexts are released. The field will contain one of the following values:

- **36**: if the SGSN sends us "delete PDP context request".
- **38**: if the GGSN sends "delete PDP context request" due to GTP-C/GTP-U echo timeout with SGSN.
- **40**: if the GGSN sends "delete PDP context request" due to receiving a RADIUS Disconnect-Request message.
- **26**: if the GGSN sends "delete PDP context request" for any other reason (e.g., the operator types "clear subscribers" on the GGSN).

duration-ms

Default: Disabled
Specifies that the information contained in the mandatory Duration field be reported in milliseconds instead of seconds (as the standards require).

dynamic-flag

Default: Enabled
Includes the Dynamic Flag field in the CDR that is created.
This keyword is applicable for P-GW and GGSN only.

imei

Default: Disabled
This keyword configures the SGSN to include the International Mobile Equipment Identifier (IM EI) in generated CDRs (M-CDRs and/or the S-CDRs).
This keyword is applicable for SGSN only.

local-record-sequence-number

Default: Disabled
Includes the Node ID field in the CDR that is created when PDP contexts are released. The field consists of a AAA Manager identifier automatically appended to the name of the GGSN or SGSN service.

The name of the GGSN/SGSN service may be truncated, because the maximum length of the Node ID field is 20 bytes. Since each AAA Manager generates CDRs independently, this allows the Local Record Sequence Number and Node ID fields to uniquely identify a CDR.

losdv

Default: Enabled
Includes the List of Service Data field in the CDR that is created.
This keyword is applicable for P-GW and GGSN only.

ms-timezone

Default: Enabled
Includes the MS-Timezone field in the CDR that is created.
This keyword is applicable for P-GW and GGSN only.

msisdn

Default: Disabled
This keyword configures the SGSN to include the Mobile Subscribers Integrated Services Digital Network identifier in generated CDRs (M-CDRs and/or the S-CDRs).
This keyword is applicable for SGSN only.

node-id

Default: Enabled
Includes the Node ID field in the CDR that is created.
This keyword is applicable for P-GW and GGSN only.

node-id-suffix *string*

Default: Disabled
Specifies the string suffix to use in the NodeID field of GTPP CDRs. Each Session Manager task generates a unique NodeID string per GTPP context.
string: This is the configured Node-ID-Suffix having any string of 1 through 16 characters.

Important: The NodeID field is a printable string of the *ndddstring* format: *n*: The first digit is the SessMgr restart counter having a value between 0 and 7. *ddd*: The number of SessMgr instances. Uses the specified NodeID-suffix in all CDRs. The "Node-ID" field is consists of SessMgr Recovery counter (1 digit) *n* + AAA Manager identifier (3 digits) *ddd* + the configured Node-Id-suffix (1 to 16 characters) *string*.

Important: If the centralized LRSN feature is enabled, the "Node-ID" field consists of only the specified NodeID-suffix. Otherwise GTPP group name is used. For default GTPP groups, GTPP context-name (truncated to 16 characters) is used.

Important: SessMgr recovery counter gets updated in case of "session recovery not enabled" If session recovery is enabled, the counter never updates. The node-id is displayed in the G-CDR irrespective of gtpp dictionary. The G-CDR is not decoded in monitor protocol for custom1 / custom3 dictionaries.

pdn-connections-id

Default: Enabled

Includes the PDN Connection ID field in the CDR that is created.
This keyword is applicable for P-GW and GGSN only.

pdp-address

Default: Enabled
Includes the PDP Address field in the CDR that is created.
This keyword is applicable for P-GW and GGSN only.

pdp-type

Default: Enabled
Includes the PDP Type field in the CDR that is created.
This keyword is applicable for P-GW and GGSN only.

pgw-plm-id

Default: Enabled
Includes the PGW PLMN-ID field in the CDR that is created.
This keyword is applicable for P-GW and GGSN only.

plmn-id [unknown-use *uncode_value* **]**

Default: Enabled
Includes the SGSN PLMN Identifier value (the RAI) in generated CDR (M-CDRs and/or the S-CDRs), if it is provided by the SGSN in the GTP create PDP context request. It is omitted if the SGSN does not supply one.

Important: For the GGSN it provides radio access identifier as the SGSN PLMN Id and for SGSN it includes the PLMN-id of RNC.

unknown-use *uncode_value* encodes the specified value for "SGSN PLMN Identifier" in the CDR if SGSN PLMN-ID information is unavailable.
Must be followed by the *uncode_value* value to be encoded.
uncode_value must be an hexadecimal value between 0x0 and 0xFFFFFF.
This keyword is applicable for SGSN only.

rat

Default: Disabled
This keyword configures the SGSN to include the radio access technology attribute in generated CDRs (M-CDRs and/or the S-CDRs).
This keyword is applicable for SGSN only.

record-extensions rat

Default: Disabled
This keyword configures the SGSN to include the radio access technology attribute in record extension field of generated CDRs (M-CDRs and/or the S-CDRs).
This keyword is applicable for SGSN only.

served-mnai

Default: Enabled
Includes the Served MNAI field in the CDR that is created.

This keyword is applicable for P-GW and GGSN only.

served-pdp-pdn-address-extension

Default: Disabled
In support of IPv4v6 dual PDP address types, this keyword causes the SGSN to include IPv4v6 address information in the S-CDR. The IPv4 address goes in the a new PDP address extension field and the IPv6 address goes in the existing servedPDPAdress field.
This keyword is applicable for SGSN only.

sms { destination-number | recording-entity | service-centre }

Default: Disabled
This keyword configures the SGSN to include the SMS related attributes in generated S-SMO-CDRs or S-SMT-CDRs.
destination-number: This keyword includes the destination-number information of SMS in generated S-SMO-CDRs or S-SMT-CDRs.
Note: This is the destination number of the short message subscriber.
recording-entity: This keyword includes the recording entity information of SMS in generated S-SMO-CDRs or S-SMT-CDRs.
Note: The recording entity is the E.164 number of the SGSN.
service-centre: This keyword includes the service-centre information of SMS in generated S-SMO-CDRs or S-SMT-CDRs.
Note: This is the E.164 address of the SMS-service centre.
This keyword is applicable for SGSN only.

start-time

Default: Enabled
Includes the Start-Time field in the CDR that is created.
This keyword is applicable for P-GW and GGSN only.

stop-time

Default: Enabled
Includes the Stop-Time field in the CDR that is created.
This keyword is applicable for P-GW and GGSN only.

uli

Default: Enabled
Includes the User Location Information field in the CDR that is created.
This keyword is applicable for P-GW and GGSN only.

Usage

Use this command to configure the type of optional information fields to include in generated CDRs (M-CDRs, S-CDRs, S-SMO-CDR, S-SMT-CDR from SGSN and G-CDRs, eG-CDRs from GGSN) by the AGW (SGSN/GGSN/P-GW). In addition, it controls how the information for some of the mandatory fields are reported.
Fields described as optional by the standards but not listed above will always be present in the CDRs, except for Record Extensions (which will never be present).

Important: This command can be repeated multiple times with different keywords to configure multiple GTPP attributes.

Example

The following command configures the system to present the time provided in the Duration field of the CDR is reported in milliseconds:

```
gtpp attribute duration-ms
```

gtpp charging-agent

Configures the IP address and port of the system interface within the current context used to communicate with the Charging Gateway Function (CGF).

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp charging-agent address *ip_address* **[port** *port* **]**

no gtpp charging-agent

no

Removes a previously configured charging agent address.

gtpp charging-agent address *ip_address*

Specifies the IP address of the interface configured within the current context that is used to transmit CDR records (G-CDR/eGCRD/M-CDR/S-CDR) to the CGF. *ip_address* must be entered using IPV4 dotted-decimal notation.

port *port*

Specifies the Charging Agent UDP port. as an integer from 1 through 65535.
If *port* is not defined, IP will take the default port number 49999.

Important: Configuring gtpp charging-agent on port 3386 may interfere with a ggsn-service configured with the same ip address.

Usage

This command establishes a Ga interface for the system. For GTPP accounting, one or more Ga interfaces must be specified for communication with the CGF. These interfaces must exist in the same context in which GTPP functionality is configured (refer to the **gtpp** commands in this chapter).
This command instructs the system as to what interface to use. The IP address supplied is also the address by which the GSN is known to the CGF. Therefore, the IP address used for the Ga interface could be identical to one bound to a GSN service (a Gn interface).
If no GSN service is configured in the same context as the Ga interface, the address configured by this command is used to receive unsolicited GTPP packets.

Example

The following command configures the system to use the interface with an IP address of *192.168.13.10* as the accounting interface with port *20000* to the CGF:

```
gtpp charging-agent address 192.168.13.10 port 20000
```

gtpp data-request sequence-numbers

Configures the range of sequence numbers to be used in the GTPP data record transfer record (DRT). Use this command to set the start value for the sequence number.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp data-request sequence-numbers start { 0 | 1 }

default gtpp data-request sequence-numbers start
```

default

Default is 0 (zero).

gtpp data-request sequence-numbers start { 0 | 1 }

Specifies the value of the start sequence number for the GTPP Data Record Transfer Request. Default: 0

- **0**: Designates the start sequence number as 0.
- **1**: Designates the start sequence number as 1.

Usage

When the GGSN/P-GW/SGSN is configured to send GTPP echo request packets, the SGSN always uses 0 as the sequence number in those packets. Re-using 0 as a sequence number in the DRT packets is allowed by the 3GPP standards; however, this CLI command ensures the possibility of inter-operating with CGFs that can not properly handle the re-use of sequence number 0 in the echo request packets.

Example

The following command sets the sequence to start at *1*.

```
gtpp data-request sequence-numbers start 1
```

gtpp dead-server suppress-cdrs

Enables or disables CDR archiving when a dead server is detected.

Important: This command is customer specific. For more information please contact your local Cisco service representative.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] gtpp dead-server suppress-cdrs
```

default

Configures the default setting.
Default: Disabled

no

Re-enables CDR archiving.

gtpp dead-server suppress-cdrs

Disables CDR archiving when a dead server is detected.

Usage

Use this command to enable/disable CDR archiving when a dead server is detected. With this CLI, once a server is detected as down, requests are purged. Also the requests generated for the period when the server is down are purged.

gtpp deadtime

Configures the amount of time to wait before attempting to communicate with a Charging Gateway Function (CGF) that was previously marked as unreachable.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

gtpp deadtime *time*

default gtpp deadtime

default

Configures this command with the default setting.
Default: 120 seconds

gtpp deadtime *time*

Specifies the amount of time (in seconds) that must elapse before the system attempts to communicate with a CGF that was previously unreachable. *time* is an integer from 1 through 65535.

Usage

If the system is unable to communicate with a configured CGF, after a pre-configured number of failures the system marks the CGF as being down.
This command specifies the amount of time that the system waits prior to attempting to communicate with the downed CGF.
Refer to the **gtpp detect-dead-server** and **gtpp max-retries** commands for additional information on the process the system uses to mark a CGF as down.

Example

The following command configures the system to wait *60* seconds before attempting to re-communicate with a CGF that was marked as down:

```
gtpp deadtime 60
```

gtpp detect-dead-server

Configures the number of consecutive communication failures that could occur before the system marks a Charging Gateway Function (CGF) as down.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

gtpp detect-dead-server consecutive-failures *max_number*

default gtpp detect-dead-server consecutive-failures

default

Configures this command with the default setting.
Default: 0

gtpp detect-dead-server consecutive-failures *max_number*

Specifies the number of failures that could occur before marking a CGF as down. *max_number* is an integer from 0 through 1000.

Usage

This command works in conjunction with the **gtpp max-retries** parameter to set a limit to the number of communication failures that can occur with a configured CGF.
The gtpp max-retries parameter limits the number of attempts to communicate with a CGF. Once that limit is reached, the system treats it as a single failure. The gtpp detect-dead-server parameter limits the number of consecutive failures that can occur before the system marks the CGF as down and communicate with the CGF of next highest priority.
If all of the configured CGFs are down, the system ignores the detect-dead-server configuration and attempt to communicate with highest priority CGF again.
If the system receives a GTPP Node Alive Request, Echo Request, or Echo Response message from a CGF that was previously marked as down, the system immediately treats it as being active.
Refer to the **gtpp max-retries** command for additional information.

Example

The following command configures the system to allow *8* consecutive communication failures with a CGF before it marks it as down:

```
gtpp detect-dead-server consecutive-failures 8
```

gtpp dictionary

Designates a dictionary used by GTPP for a specific context.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp dictionary { custom1 | custom10 | custom11 | custom12 | custom13 | custom14 |
custom15 | custom16 | custom17 | custom18 | custom19 | custom2 | custom20 | custom21 |
custom22 | custom23 | custom24 | custom25 | custom26 | custom27 | custom28 | custom29 |
custom3 | custom30 | custom31 | custom32 | custom33 | custom34 | custom35 | custom36 |
custom37 | custom38 | custom39 | custom4 | custom40 | custom41 | custom42 | custom43 |
custom44 | custom45 | custom46 | custom47 | custom48 | custom49 | custom5 | custom50 |
custom51 | custom52 | custom53 | custom54 | custom55 | custom56 | custom57 | custom58 |
custom59 | custom6 |  custom60 | custom7 | custom8 | custom9 | standard }

default gtpp dictionary
```

default

Configures the default dictionary.

custom1

This is a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99. It supports the encoding of IP addresses in text format for G-CDRs.

custom2

Custom-defined dictionary.

custom3

This is a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99 except that it supports the encoding of IP addresses in binary format for G-CDRs.

custom4

This is a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99 except that:

- IP addresses are encoded in binary format.
- The Data Record Format Version information element contains 0x1307 instead of 0x1308.
- QoSRequested is not present in the LoTV containers.
- QoSnegotiated is added only for the first container and the container after a QoS change.

custom5

Custom-defined dictionary.

custom6

This is a custom-defined dictionary for eG-CDR encoding.

custom7 ... custom30

These custom-defined dictionary have default behavior or "standard" dictionary.

custom31

This is a custom-defined dictionary for S-CDR encoding that is based on 3GPP TS 32.298 v6.4.1 with a special field appended for the PLMN-ID.

custom33

This ia a custom-defined dictionary for S-CDR encoding that is based on the 3GPP TS 32.298 v6.4.1 with the following exceptions:

- Proprietary PLMN-ID field is present.
- It is a SEQUENCE and not a SET.
- Diagnostics and SGSN-Change fields are not supported.
- Indefinite length encoding is used.
- Booleans are encoded as 0x01(3GPP it is 0xff).
- IMEISV shall be sent if available else IMEI should be sent.
- Record Sequence Number is Mandatory.
- APN OI and NI part is length encoded.
- Cause for Record closure should be "RAT Change" instead of "intra-SGSN inter-system".

standard

Default: Enabled
This dictionary conforms to TS 32.215 v 4.6.0 for R4 (and also R5 - extended QoS format).

Usage

Use this command to designate specific dictionary used by GTPP for specific context.

Example

The following command configures the system to use *custom3* dictionary to encode IP address in Binary format in G-CDRs:

```
gtpp dictionary custom3
```

gtpp duplicate-hold-time

Configures the number of minutes to hold onto CDRs that are possibly duplicates while waiting for the primary Charging Gateway Function (CGF) to come back up.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp duplicate-hold-time *minutes*

default gtpp duplicate-hold-time

default

Configures this command with the default setting.
Default: 60 minutes

gtpp duplicate-hold-time *minutes*

Specifies the number of minutes to hold onto CDRs that may be duplicates whenever the primary CGF is down, *minutes* must be an integer from 1 through 10080.

Usage

Use this command to configure how long to hold onto CDRs that are possibly duplicates while waiting for the primary CGF to come back up. If the GGSN/P-GW determines that the primary CGF is down, CDRs that were sent to the primary CGF but not acknowledged are sent by the GSN to the secondary CGF as "possibly duplicates". When the primary CGF comes back up, the GSN uses GTPP to determine whether the possibly duplicate CDRs were received by the primary CGF. Then the secondary CGF is told whether to release or cancel those CDRs. This command configures how long the system should wait for the primary CGF to come back up. As soon as the configured time expires, the secondary CGF is told to release all of the possibly duplicate CDRs.

Example

Use the following command to set the amount of time to hold onto CDRs to 2 hours (120 minutes);

```
gtpp duplicate-hold-time 120
```

gtpp echo-interval

Configures the frequency at which the system sends GTPP echo packets to configured CGFs.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp echo-interval time

{ default | no } gtpp echo-interval
```

default

Configures the default setting for this command,
Default: 60 seconds

no

Disables the use of the echo protocol except for the scenarios described in the *Usage* section for this command.

gtpp echo-interval *time*

Specifies the time interval (in seconds) for sending GTPP echo packets as an integer from 60 through 2147483647. Default: 60

Usage

The GTPP echo protocol is used by the system to ensure that it can communicate with configured CGFs. The system initiates this protocol for each of the following scenarios:

- Upon system boot
- Upon the configuration of a new CGF server on the system using the **gtpp server** command as described in this chapter
- Upon the execution of the **gtpp test accounting** command as described in the *Exec Mode Commands* chapter of this reference
- Upon the execution of the **gtpp sequence-numbers private-extensions** command as described in this chapter

The echo-interval command is used in conjunction with the gtpp max-retries and gtpp timeout commands as described in this chapter.
In addition to receiving an echo response for this echo protocol, if we receive a GTPP Node Alive Request message or a GTPP Echo Request message from a presumed dead CGF server, we will immediately assume the server is active again.
The alive/dead status of the CGFs is used by the AAA Managers to affect the sending of CDRs to the CGFs. If all CGFs are dead, the AAA Managers will still send CDRs, (refer to the **gtpp deadtime** command), albeit at a slower rate than if a CGF were alive. Also, AAA Managers independently determine if CGFs are alive/dead.

Example

The following command configures an echo interval of *120* seconds:

```
gtpp echo-interval 120
```

gtpp egcdr

Configures the eG-CDR and P-CDR (P-GW CDR) parameters and triggers.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
gtpp egcdr { final-record [ [ include-content-ids { all | only-with-traffic } ] [
closing-cause { same-in-all-partials | unique } ] ] | losdv-max-containers
max_losdv_containers | lotdv-max-containers max_lotdv_containers | rulebase-max-length
rulebase_name_max_length | service-data-flow threshold { interval interval | volume {
downlink bytes [ uplink bytes ] | total bytes | uplink bytes [ downlink bytes ] } } |
service-idle-timeout { 0 | service_idle_timeout } }

default gtpp egcdr { final-record include-content-ids only-with-traffic closing-cause
same-in-all-partials | losdv-max-containers | lotdv-max-containers | service-idle-timeout
0 }

no gtpp egcdr { rulebase-max-length | service-data-flow threshold { interval | volume {
downlink [ uplink ] | total | uplink [ downlink ] } } }
```

final-record [[include-content-ids { all | only-with-traffic }] [closing-cause { same-in-all-partials | unique }]]

Enables configuration of the final eG-CDR/P-CDR.
Default: Restores the GTPP eG-CDR/P-CDR final record to the default setting to include content IDs with some data to report are included. Also, sets the closing cause to the default of using the same closing cause for multiple final eG-CDR/P-CDRs.

- **include-content-ids**: Controls which content IDs are being included in the final eG-CDR/P-CDR.
  - **all**: Specifies that all content IDs be included in the final eG-CDR/P-CDR.
  - **only-with-traffic**: Specifies that only content-IDs with traffic be included in the final eG-CDR/P-CDRs.
- **closing-cause**: Configures closing cause for the final eG-CDR/P-CDR.
  - **same-in-all-partials**: Specifies that the same closing cause is to be included for multiple final eG-CDR/P-CDRs
  - **unique**: Specifies that the closing cause for final eG-CDR/P-CDRs is to be unique.

losdv-max-containers *max_losdv_containers*

The maximum number of List of Service Data Volume (LoSDV) containers in one eG-CDR/P-CDR.
max_losdv_containers must be an integer from 1 through 255.
Default: 10

lotdv-max-containers *max_lotdv_containers*

The maximum number of List of Traffic Data Volume (LoTDV) containers in one eG-CDR/P-CDR.
max_lotdv_containers must be an integer from 1 through 8.

Default: 8

rulebase-max-length *rulebase_name_max_length*

Specifies the maximum character length of charging rulebase name in LOSDVs of eG- CDR/P-CDR.
rulebase_name_max_length must be an integer from 0 through 63. Zero (0) means the rulebase name is added as-is.
Default: None. That is, full (un-truncated) charging rulebase name will go in LOSDVs of eG-CDR/P-CDR.

service-data-flow threshold { interval *interval* **| volume { downlink** *bytes* **[uplink** *bytes* **] | total** *bytes* **| uplink** *bytes* **[downlink** *bytes* **] } }**

Configures the thresholds for closing a service data flow container within an eG-CDR/P-CDR.

- **interval** *interval*: Specifies the time interval, in seconds, to close the eG-CDR/P-CDR if the minimum time duration thresholds for service data flow containers satisfied in flow-based charging.

  interval must be an integer from 60 through 40000000.

  Default: Disabled

- **volume { downlink** *bytes* **[uplink** *bytes* **] | total** *bytes* **| uplink** *bytes* **[downlink** *bytes* **] }**: Specifies the volume octet counts for the generation of the interim eG-CDR/P-CDRs to service data flow container in FBC.

  - **downlink** *bytes*: Specifies the limit for the number of downlink octets after which the eG-CDR/P-CDR is closed.
  - **total** *bytes*: Specifies the limit for the total number of octets (uplink+downlink) after which the eG-CDR/P-CDR is closed.
  - **uplink** *bytes*: Specifies the limit for the number of uplink octets after which the eG-CDR/P-CDR is closed.
  - *bytes* must be an integer from 10000 through 400000000.

A service data flow container has statistics for an individual content ID. When the threshold is reached, the service data flow container is closed.

service-idle-timeout { 0 | *service_idle_timeout* **}**

Specifies a time period where if no data is reported for a service flow, the service container is closed and added to eG-CDR/P-CDR (as part of LOSDV container list) with service condition change as ServiceIdleOut.
service_idle_timeout must be an integer from 10 through 86400.
0: Specifies no service-idle-timeout trigger.
Default: 0

Usage

Use this command to configure individual triggers for eG-CDR/P-CDR generation.
Use the **service-data-flow threshold** option to configure the thresholds for closing a service data flow container within an eG-CDR (eG-CDRs for GGSN and P-CDRs for PGW) during flow-based charging (FBC). A service data flow container has statistics regarding an individual content ID.
Thresholds can be specified for time interval and for data volume, by entering the command twice (once with interval and once with volume). When either configured threshold is reached, the service data flow container will be closed. The volume trigger can be specified for uplink or downlink or the combined total (uplink + downlink) byte thresholds.
When the PDP context is terminated, all service data flow containers will be closed regardless of whether the thresholds have been reached.

An eG-CDR/P-CDR will have at most ten service data flow containers. Multiple eG-CDR/P-CDRs will be created when there are more than ten.

Example

Use the following command to set the maximum number of LoSDV containers to *7*:

```
gtpp egcdr losdv-max-containers 7
```

The following command sets an eG-CDR threshold interval of *6000* seconds:

```
gtpp egcdr service-data-flow threshold interval 6000
```

gtpp error-response

Configures the response when the system receives an error response after transmitting a DRT (data record transfer) request.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp error-response { discard-cdr | retry-request }

default gtpp error-response
```

default

Configures this command with the default setting.
Default: **retry-request**

gtpp error-response discard-cdr

Instructs the system to purge the request upon receipt of an error response and not to retry.

gtpp error-response retry-request

Instructs the system to retry sending a DRT after receiving an error response. This is the default behavior.

Usage

This command configures the system's response to receiving an error message after sending a DRT request.

Example

```
gtpp error-response discard-cdr
```

gtpp group

Configures GTPP server group in a context for the Charging Gateway Function (CGF) accounting server(s) that the system is to communicate with.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] gtpp group *group_name* **[-noconfirm]**

gtpp group *group_name*

Specifies the name of GTPP server group that is used for charging and/or accounting in a specific context.
group_name must be an alphanumeric string of 1 through 63 character.
A maximum of eight GTPP server groups (excluding system created default GTPP server group "default") can be configured with this command in a context.

no

Removes the previously configured GTPP group within a context.
When a GTPP group is removed accounting information is not generated for all calls using that group and all calls associated with that group are dropped. A warning message displays indicating the number of calls that will be dropped.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

This feature provides the charging gateway function (CGF) accounting server configurable for a group of servers. Instead of having a single list of CGF accounting servers per context, this feature configures multiple GTPP accounting server groups in a context and each server group is consist of list of CGF accounting servers.
In case no GTPP server group is configured in a context, a server group named "default" is available and all the CGF servers configured in a specific context for CGF accounting functionality will be part of this "default" server group.

Example

The following command configures a GTPP server group named *star1* for CGF accounting functionality. This server group is available for all subscribers within that context.

```
gtpp group star1
```

gtpp max-cdrs

Configures the maximum number of charging data records (CDRs) included per packet.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp max-cdrs *max_cdrs* **[wait-time** *wait_time* **]**

default gtpp max-cdrs

default

Configures this command with the default setting.
Default: One CDR per packet; disables **wait-time**

gtpp max-cdrs *max_cdrs*

Specifies the maximum number of CDRs to be inserted in a single packet as an integer from 1 through 255.
Default: 1

wait-time *wait_time*

Specifies the number of seconds the system waits for CDRs to be inserted into the packet before sending it. *wait_time* must be an integer from 1 through 300. Default: Disabled

Important: If the **wait-time** expires, the packet is sent as this keyword over-rides *max_cdrs*.

Usage

CDRs are placed into a GTPP packet as the CDRs close. The system stops placing CDRs into a packet when either the maximum *max_cdrs* is met, or the **wait-time** expires, or the value for the **gtpp max-pdu-size** command is met.

Example

The following command configures the system to place a maximum of *10* CDRs in a single GTPP packet before transmitting the packet:

```
gtpp max-cdrs 10
```

gtpp max-pdu-size

Configures the maximum payload size of a single GTPP packet that could be sent by the system.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp max-pdu-size *pdu_size*

default gtpp max-pdu-size

default

Configures this command with the default setting.
Default: 65400 bytes

gtpp max-pdu-size *pdu_size*

Specifies the maximum payload size (in octets) of the GTPP packet as an integer from 1024 to 65400. The payload includes the CDR and the GTPP header.

Caution: This command is effective only when GTPP single-source is configured, otherwise this command has no effect.

Usage

The GTPP packet contains headers (layer 2, IP, UDP, and GTPP) followed by the CDR. Each CDR contains one or more volume containers. If a packet containing one CDR exceeds the configured maximum payload size, the system creates and send the packet containing the one CDR regardless.
The larger the packet data unit (PDU) size allowed, the more volume containers that can be fit into the CDR. The system performs standard IP fragmentation for packets that exceed the system's maximum transmission unit (MTU).

Important: The maximum size of an IPv4 PDU (including the IPv4 and subsequent headers) is 65,535. However, a slightly smaller limit is imposed by this command because the system's max-pdu-size doesn't include the IPv4 and UDP headers, and because the system may need to encapsulate GTPP packets in a different/larger IP packet (for sending to a backup device).

Example

The following command configures a maximum PDU size of *2048* octets:

```
gtpp max-pdu-size 2048
```

gtpp max-retries

Configures the maximum number of times the system attempts to communicate with an unresponsive Charging Gateway Function (CGF).

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp max-retries *max_attempts*

default gtpp max-retries

default

Configures this command with the default setting.
Default: 4

gtpp max-retries *max_attempts*

Specifies the number of times the system attempts to communicate with a CGF that is not responding. *max_attempts* is an integer from 1 through 15.

Usage

This command works in conjunction with the **gtpp detect-dead-server** and **gtpp timeout** parameters to set a limit to the number of communication failures that can occur with a configured CGF.
When the value specified by this parameter is met, a failure is logged. The gtpp detect-dead-server parameter specifies the number of consecutive failures that could occur before the server is marked as down.
In addition, the gtpp timeout command controls the amount of time between re-tries.
If the value for the max-retries is met, the system begins storing CDRs in Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context). Archived CDRs are re-transmitted to the CGF until they are acknowledged or the system's memory buffer is exceeded.
Refer to the **gtpp detect-dead-server** and **gtpp timeout** commands for additional information.

Example

The following command configures the maximum number of re-tries to be *8*:

```
gtpp max-retries 8
```

gtpp node-id

Configures the GTPP Node ID for all CDRs.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp node-id *node_id*

no gtpp node-id

no

Removes the previous gtpp node ID configuration.

gtpp node-id *node_id*

Specifies the node ID for all CDRs as an alphameric string of 1 through 16 characters.

Usage

Use this command to configure the GTPP Node ID for all CDRs.

Example

The following command configures the GTPP Node ID as *test123*:

```
gtpp node-id test123
```

gtpp redirection-allowed

Configures the system to allow or disallow the redirection of CDRs when the primary Charging Gateway Function (CGF) is unavailable.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp redirection-allowed

{ default | no } gtpp redirection-allowed
```

default

Configures this command with the default setting. Default: Enabled

no

Deletes the command from the configuration.

gtpp redirection-allowed

Allows the redirection of CDRs when the primary Charging Gateway Function (CGF) is unavailable.

Usage

This command allows operators to better handle erratic network links, without having to remove the configuration of the backup server(s) via the **no gtpp server** command.
This functionality is enabled by default.
If the no gtpp redirection-allowed command is executed, the system only sends CDRs to the primary CGF. If that CGF goes down, we will buffer the CDRs in memory until the CGF comes back or until the system runs out of buffer memory. In addition, if the primary CGF announces its intent to go down (with a GTPP Redirection Request message), the system responds to that request with an error response.

gtpp redirection-disallowed

This command has been obsoleted and is replaced by the **gtpp redirection-allowed** command.

gtpp server

Configures the Charging Gateway Function (CGF) accounting server(s) with which the system will communicate.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp server *ip_address* [**max** *max_messages*] [**priority** *priority*] [**udp-portport** *port*] [**node-alive** { **enable** | **disable** }] [**-noconfirm]**

no gtpp server *ip_address*

---

no

Deletes a previously configured CGF.

---

gtpp server *ip_address*

Specifies the IP address of the CGF in IPv4 dotted-decimal or IPV6 colon-separated notation.

---

max *max_messages*

Default: 256
Specifies the maximum number of outstanding or unacknowledged GTPP packets (from any one AAA Manager task) allowed for this CGF before the system begins buffering the packets.
max_messages can be configured as an integer from 1 through 256.

---

priority *priority*

Default:1000
Specifies the relative priority of this CGF. When multiple CGFs are configured, the priority is used to determine which CGF server to send accounting data to.
priority can be configured as an integer from 1 through 1000. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the **-noconfirm** option, you are not asked for confirmation and multiple servers could be assigned the same priority.

---

udp-port *port*

Default: 3386
Specifies the UDP port the CGF is using. *port* can be configured as an integer from 1 through 65535.
Default value for port is 3286.

Important: The **udp-port** keyword option has been modified to **port** to make it a generic command. The **udp-port** keyword can still be used, however it will be in concealed mode and will not be shown in auto-complete or help for the command.

---

node-alive { enable | disable }

Default: Disable.

This optional keyword allows operator to enable/disable GSN to send Node Alive Request to GTPP Server (i.e. CGF). This configuration can be done per GTPP Server basis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to configure the CGF(s) that the system sends CDR accounting data to. Multiple CGFs can be configured using multiple instances of this command. Up to 12 CGFs can be configured per system context. Each configured CGF can be assigned a priority. The priority is used to determine which server to use for any given subscriber based on the routing algorithm that has been implemented. A CGF with a priority of "1" has the highest priority.

Important: The configuration of multiple CGFs with the same IP address but different port numbers is not supported.

Each CGF can also be configured with the maximum allowable number of unacknowledged GTPP packets. Since multiple AAA Manager tasks could be communicating with the same CGF, the maximum is based on any one AAA Manager instance. If the maximum is reached, the system buffers the packets Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context).

Example

The following command configures a CGF with an IP address of *192.168.2.2* and a priority of *5*.

```
gtpp server 192.168.2.2 priority 5
```

The following command deletes a previously configured CGF with an IP address of *100.10.35.7*:

```
no gtpp server 100.10.35.7
```

gtpp source-port-validation

Toggles port checking for node alive/echo/redirection requests from the CGF.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
gtpp source-port-validation

{ no | default } gtpp source-port-validation
```

no

Disables CGF port checking. Only the IP address will be used to verify CGF requests.

default

Configures this command with the default setting.
Default: Enabled

gtpp source-port-validation

Enables port checking for node alive/echo/redirection requests from the CGF.

Usage

This command is for enabling or disabling port checking on node alive/echo/redirection requests from the CGF. If the CGF sends messages on a non-standard port, it may be necessary to disable port checking in order to receive CGF requests. On the default setting, both IP and port are checked.

Example

The following command disables port checking for CGF requests:

```
no gtpp source-port-validation
```

gtpp storage-server

Configures information for the GTPP back-up storage server.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp storage-server *ip-address* **port** *port-num*

no gtpp storage-server *ip-address* **port** *port-num*

no

Removes a previously configured back-up storage server.

gtpp storage-server *ip-address*

Specifies the IP address of the back-up storage server expressed in IPv4 dotted-decimal notation.

port *port-num*

Specifies the UDP port number over which the GSN communicates with the back-up storage server. Default: 3386

Usage

This command configures the information for the server to which GTPP packets are to be backed-up to in the event that all CGFs are unreachable.
One backup storage server can be configured per system context.

Important: This command only takes affect if **gtpp single-source** in the Global Configuration Mode is also configured. Additionally, this command is customer specific. Please contact your local sales representative for additional information.

Example

The following command configures a back-up server with an IP address of *192.168.1.2*:

```
gtpp storage-server 192.168.1.2
```

gtpp storage-server local file

Configures the parameters for GTPP files stored locally on the GTPP storage server. This command is available for the ASR 5000 platform only.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp storage-server local file { **compression** { **gzip** | **none** } | **format** { **custom1** | **custom2** | **custom3** | **custom4** | **custom5** | **custom6** | **custom7** | **custom8** } | **name** { **format** *string* [**max-file-seq-num** *seq_number*] | **prefix** *prefix* } | **purge-processed-files** [**file-name-pattern** *file_pattern* | **purge-interval** *purge_dur*] | **rotation** { **cdr-count** *count* | **time-interval** *time* [**force-file-rotation**] | **volume mb** *size* } | **start-file-seq-num** *seq_num* [**recover-file-seq-num**] }

default gtpp storage-server local file { **compression** | **format** | **name** { **format** | **prefix** } | **purge-processed-files** | **rotation** { **cdr-count** | **time-interval** | **volume** } | **start-file-seq-num** }

no gtpp storage-server local file { **purge-processed-files** | **rotation** { **cdr-count** | **time-interval** } }

---

default

Configures default setting for the specified parameter.

---

no

Removes a previously configured parameters for local storage of CDR files on HDD on SMC card.

---

compression { gzip | none }

Configures the type of compression to be used on the files stored locally.

- **gzip**: Enables Gzip file compression.
- **none**: Disables Gzip file compression -this is the default value.

Default: Disabled

---

format { *custom-n* **}**

Configures the file format to be used to format files to be stored locally.
custom1: File format custom1—this is the default value.
custom2: File format custom2.
custom3: File format custom3.
custom4: File format custom4.
custom5: File format custom5.
custom6: File format custom6 with a block size of 8K for CDR files.
custom7: File format custom7 is a customer specific CDR file format.
custom8: File format custom8 is a customer specific CDR file format. It uses *node-id-suffix_date_time_fixed-length-seq-num*.u format for file naming.

Default: **custom1**

name { format | prefix *prefix* **}**

Allows the format of the CDR filenames to be configured independently from the file format.so that the name format contains the file name with conversion specifications.
prefix – Enter an alphanumeric string of 1 through 127 characters. The string **must begin** with the % (percent sign).

- **%y**: = year as a decimal number without century (range 00 to 99).
- **%Y**: year as a decimal number with century.
- **%m**: month as a decimal number (range 01 to 12).
- **%d**: day of the month as a decimal number (range 01 to 31).
- **%H**: hour as a decimal number 24-hour format (range 00 to 23).
- **%h**: hour as a decimal number 12-hour format (range 01 to 12).
- **%M**: minute as a decimal number (range 00 to 59).
- **%S**: second as a decimal number (range 00 to 60). (The range is up to 60 to allow occasional leap seconds.)
- **%Q**: File sequence number. Field width may be specified between the % and the Q. If the natural size of the field is smaller than this width, then the result string is padded (on the left) to the specified width with 0s
- **%N**: No of CDRs in the file. Field width may be specified between the % and the N. If the natural size of the field is smaller than this width, then the result string is padded (on the left) to the specified width with 0s
- **max-file-seq-no**: This can be configured optionally. It indicates the maximum value of sequence number in file name (starts from 1). Once the configured max-file-seq-no limit is reached, the sequence number will restart from 1. If no max-file-seq-no is specified then file sequence number ranges from 1 – 4294967295.

By default the above keyword is not configured (default gtpp storage-server local file name format). In which case the CDR filenames are generated based on the file format as before (maintains backward compatibility).

purge-processed-files [file-name-pattern *file_pattern* **| purge-interval** *purge_dur* **]**

Enables the GSN to periodically (every 4 minutes) delete locally processed (*.p) CDR files from the HDD on the SMC card. Default: Disabled

Important: This option is available only when GTPP server storage mode is configured for local storage of CDRs with the **gtpp storage-server mode local** command.

Optional keyword **file-name-pattern** *file_pattern* provides an option for user to control the pattern of files. *file_pattern* must be mentioned in *.p format in a string of size 1 through 127, which is also the default format. Wild cards * and : (synonymous to |) are allowed.
Optional keyword **purge-interval** *purge_dur* provides an option for user to control the purge interval duration (in minutes). *purge_dur* must be an integer from 1 through 259200. Default value 60.

rotation { cdr-count count | time-interval *time* **| volume mb** *size* **}**

Specifies rotation related configuration for GTPP files stored locally.

cdr-count *count*: Configures the CDR count for the file rotation as an integer from 1000 through 65000. Default value 10000.
time-interval *time*: Configures the time interval (in seconds) for file rotation as an integer from 30 through 86400. Default value 3600 (1 hour).
volume mb *size*: Configure the file volume (in MB) for file rotation. Enter an integer from 2 to 40. This trigger cannot be disabled. Default value is 4MB.

start-file-seq-num *seq_num* **[recover-file-seq-num]**

Specifies the start sequence number. The sequence number goes on incrementing until ULONG_MAX (or max-seq-num configured in file name format) and then it would rollover. If **recover-file-seq-num** is configured, every time the system is rebooted (or aaaproxy recovery/ planned/ unplanned packet service card migration), the file sequence number continues from the last sequence number and during rollover it starts from first-sequence number.
seq_num: Configures the sequence number. Enter an integer from 1 through 4294967295.
recover-file-seq-num: Configures the recovery of file sequence number. This is an optional field and if configured, every time the machine rebooted, the file sequence number continues from the last sequence number.

Usage

This command configures the parameters for storage of GTPP packets as files on the local server—meaning the hard disk.

Example

The following command configures rotation for every 1.5 hours (5400 seconds) for locally stored files.

```
gtpp storage-server local file rotation time-interval 5400 start-file-
seq-num 20 recover-file-seq-num
```

gtpp storage-server max-retries

Configures the maximum number of times the system attempts to communicate with an unresponsive GTPP back-up storage server.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

gtpp storage-server max-retries *max_attempts*

default gtpp storage-server max-retries

default

Configures this command with the default setting.
Default: 2

gtpp storage-server max-retries *max_attempts*

Specifies the number of times the system attempts to communicate with a GTPP back-up storage server that is not responding. *max_attempts* enter an integer from 1 through 15.

Usage

This command works in conjunction with the **gtpp storage-server timeout** parameters to set a limit to the number of communication failures that can occur with a configured GTPP back-up storage server.
The **gtpp storage-server timeout** command controls the amount of time between re-tries.

Example

The following command configures the maximum number of re-tries to be *8*:

```
gtpp storage-server max-retries 8
```

gtpp storage-server mode

Configures storage mode, local or remote, for CDRs. Local storage mode is available with ASR 5000 platforms only.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp storage-server mode { local | remote | streaming }

default gtpp storage-server mode
```

default

Configures this command with the default setting.
Default: **remote**

gtpp storage-server mode local

Default: Disabled
Specifies the use of the hard disk on the SMC for storing CDRs

gtpp storage-server mode remote

Specifies the use of an external server for storing CDRs. This is the default value.

gtpp storage-server mode streaming

Default: Disabled
Allows the operator to configure "streaming" mode of operation for GTPP group. When this keyword is supplied the CDRs will be stored in following fashion:

- When GTPP link is active with CGF, CDRs are sent to a CGF via GTPP and local hard disk is NOT used as long as every record is acknowledged in time.
- If the GTPP connection is considered to be down, all streaming CDRs will be saved temporarily on the local hard disk and once the connection is restored, unacknowledged records will be retrieved from the hard disk and sent to the CGF.

Usage

This command configures whether the CDRs should be stored on the hard disk of the SMC or remotely, on an external server.

Example

The following command configures use of a hard disk for storing CDRs:

```
gtpp storage-server mode local
```

gtpp storage-server timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the GTPP back-up storage server.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

gtpp storage-server timeout *duration*

default gtpp storage-server timeout

default

Configures this command with the default setting.
Default: 30 seconds

gtpp storage-server timeout *duration*

Specifies the maximum amount of time (in seconds) the system waits for a response from the GTPP back-up storage server before assuming the packet is lost. *duration* is an integer from 30 through 120.

Usage

This command works in conjunction with the **gtpp storage-server max-retries** command to establish a limit on the number of times that communication with a GTPP back-up storage server is attempted before a failure is logged. This parameter specifies the time between retries.

Example

The following command configures a retry timeout of *60* seconds:

```
gtpp storage-server timeout 60
```

gtpp suppress-cdrs zero-volume-and-duration

Suppresses the CDRs created by sessions having zero duration and/or zero volume. By default this mode is disabled.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp suppress-cdrs zero-volume-and-duration { gcdrs [ egcdrs ] | egcdrs [ gcdrs ] }

default gtpp suppress-cdrs zero-volume-and-duration
```

default

Configures this command with the default setting.
Default: Disabled.

gtpp suppress-cdrs zero-volume-and-duration gcdrs [egcdrs]

Suppresses G-CDRs before eG-CDRs.

gtpp suppress-cdrs zero-volume-and-duration egcdrs [gcdrs]

Suppresses eG-CDRs before G-CDRs.

Usage

Use this command to suppress the CDRs (G-CDRs and eG-CDRs) which were created when zero-duration sessions and zero-volume sessions are encountered due to any reason. By default this command is disabled and system will not suppress any CDR.

Example

The following command configures the system to suppress the eG-CDRs created for a zero duration session or zero volume session:

```
gtpp suppress-cdrs zero-volume-and-duration egcdrs gcdrs
```

gtpp timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the Charging Gateway Function (CGF).

Product

GGSN, SGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

gtpp timeout *time*

default gtpp timeout

default

Configures this command with the default setting. Default: 20 seconds

gtpp timeout *time*

Specifies the maximum amount of time (in seconds) the system waits for a response from the CGF before assuming the packet is lost. *time* is an integer from 1 through 60.

Usage

This command works in conjunction with the **gtpp max-retries** command to establish a limit on the number of times that communication with a CGF is attempted before a failure is logged.
This parameter specifies the time between retries.

Example

The following command configures a retry timeout of *30* seconds:

```
gtpp timeout 30
```

gtpp trigger

This command is left in place for backward compatibility. To disable and enable GTPP triggers you should use the **gtpp trigger** command in GTPP Server Group Configuration Mode.

gtpp transport-layer

Selects the transport layer protocol for the Ga interface for communication between the access gateways (GSNs) and GTPP servers.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp transport-layer { tcp | udp }

default gtpp transport-layer
```

default

Configures this command with the default setting.
Default: **udp**

gtpp transport-layer tcp

Default: Disabled
Enables the system to implement TCP as transport layer protocol for communication with GTPP server.

gtpp transport-layer udp

Default: Enabled
Enables the system to implement UDP as transport layer protocol for communication with GTPP server.

Usage

Use this command to select the TCP or UDP as the transport layer protocol for Ga interface communication between GTPP servers and AGWs (GSNs).

Example

The following command enables TCP as the transport layer protocol for the GSN's Ga interface.

```
gtpp transport-layer tcp
```

gtpu-service

Creates a GTP-U service or specifies an existing GTP-U service and enters the GTP-U Service Configuration Mode for the current context.

Product

GGSN, P-GW, S-GW

Privilege

Administrator

Syntax

gtpu-service *service_name* **[-noconfirm]**

no gtpu-service *service_name*

gtpu-service *service_name*

Specifies the name of the GTP-U service. If *service_name* does not refer to an existing service, a new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no gtpu-service *service_name*

Removes the specified GTP-U service from the context.

Usage

Enter the GTP-U Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-gtpu-service)#
```

GTP-U Service Configuration Mode commands are defined in the *GTP-U Service Configuration Mode Commands* chapter.

Example

The following command enters the existing GTP-U Service Configuration Mode (or creates it if it does not already exist) for the service named *gtpu-service1*:

```
gtpu-service gtpu-service1
```

The following command will remove *gtpu-service1* from the system:

```
no gtpu-service gtpu-service1
```

ha-service

Creates/deletes a home agent service or specifies an existing HA service for which to enter the Home Agent Service Configuration Mode for the current context.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

ha-service *name*

no ha-service *name*

no

Indicates the home agent service specified is to be removed.

ha-service *name*

Specifies the name of the HA service to configure. If *name* does not refer to an existing service, the new service is created if resources allow. *name* is an alphanumeric string of 1 through 63 characters.

Usage

Enter the HA Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

The following command will enter, or create and enter, the HA service *sampleService*:

```
ha-service sampleService
```

The following command will remove *sampleService* as being a defined HA service:

```
no ha-service sampleService
```

hnbgw-service

Creates or removes an Home NodeB Gateway (HNB-GW) service or configures an existing HNB-GW service and enters the HNB-GW Service Configuration Mode for Femto UMTS access networks configuration in the current context.

Product

HNB-GW

Privilege

Administrator

Syntax

hnbgw-service *hnbgw_svc_name* **[-noconfirm]**

no hnbgw-service *hnbgw_svc_name*

no

Removes the specified HNB-GW service from the context.

hnbgw-service *hnbgw_svc_name*

Specifies the name of the HNB-GW service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *hnbgw_svc_name* is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to enter the HNB-GW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of one HNB-GW service which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-hnbgw-service)#
```

The commands available in this mode are defined in the *HNB-GW Service Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Caution: This is a critical configuration. The HNB-GW service can not be configured without this configuration. Any change to this configuration would lead to restarting the HNB-GW service and removing or disabling this configuration will stop the HNB-GW service.

Example

The following command enters the existing HNB-GW Service Configuration Mode (or creates it if it does not already exist) for the service named *hnb-service1*:

```
hnbgw-service hnb-service1
```

The following command will remove *hnb-service1* from the system:

```
no hnbgw-service hnb-service1
```

hsgw-service

Creates an HSGW service or specifies an existing HSGW service and enters the HSGW Service Configuration Mode for the current context.

Product

HSGW

Privilege

Administrator

Syntax

hsgw-service *service_name* **[-noconfirm]**

no hsgw-service *service_name*

hsgw-service *service_name*

Specifies the name of the HSGW service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no hsgw-service *service_name*

Removes the specified HSGW service from the context.

Usage

Enter the HSGW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-hsgw-service)#
```

HSGW Service Configuration Mode commands are defined in the *HSGW Service Configuration Mode Commands* chapter.
Use this command when configuring the following eHRPD components: HSGW.

Example

The following command enters the existing HSGW Service Configuration Mode (or creates it if it does not already exist) for the service named *hsgw-service1*:

```
hsgw-service hsgw-service1
```

The following command will remove *hsgw-service1* from the system:

```
no hsgw-service hsgw-service1
```

hss-peer-service

Creates a Home Subscriber Service (HSS) peer service or configures an existing HSS peer service and enters the HSS Peer Service Configuration Mode.

Product

MME

Important: For an SGSN, this command is visible, but the feature is in development and not yet supported for configuration.

Privilege

Administrator

Syntax

hss-peer-service *service_name* **[-noconfirm]**

no hss-peer-service *service_name*

no mme-hss-service *service_name*

Removes the specified HSS peer service from the context.

hss-peer-service *service_name*

Specifies the name of the HSS peer service. If *service_name* does not refer to an existing service, a new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Enter the HSS Peer Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-hss-peer-service)#
```

HSS Peer Service Configuration Mode commands are defined in the *HSS Peer Service Configuration Mode Commands* chapter.

Example

The following command enters the existing HSS Peer Service Configuration Mode (or creates it if it does not already exist) for the service named *hss-peer1*:

```
hss-peer-service hss-peer1
```

The following command will remove *hss-peer1* from the system:

```
no hss-peer-service hss-peer1
```

ikev1 disable-initial-contact

Disables the sending of the INITIAL-CONTACT message in the IKEv1 protocol after the node creates a new Phase1 SA, caused either by Dead Peer Detection or by a rekey.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ikev1 disable-initial-contact
```

no

Disables this command, which re-enables the sending of the INITIAL-CONTACT message.

ikev1 disable-initial-contact

Enables the sending of the INITIAL-CONTACT message.

Usage

Use this command to disable the sending of the INITIAL-CONTACT message in the IKE v1 protocol.

Example

The following command disables the sending of the INITIAL-CONTACT message:

```
ikev1 disable-initial-contact
```

ikev1 disable-phase1-rekey

Configures the rekeying of Phase1 SA when the Internet Security Association and Key Management Protocol (ISAKMP) lifetime expires in Internet Key Exchange (IKE) v1 protocol.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ikev1 disable-phase1-rekey
```

no

Re-enables Phase 1 SAs when the ISAKMP lifetime expires.

ikev1 disable-phase1-rekey

Rekeys the Phase 1 SAs when the ISAKMP lifetime expires.

Usage

Use this command to disable the rekeying of Phase 1 SAs when the ISAKMP lifetime expires in IKE v1 protocol.

Example

The following command disables rekeying of Phase1 SAs when the lifetime expires:

```
ikev1 disable-phase1-rekey
```

ikev1 keepalive dpd

Configures the ISAKMP IPSec Dead Peer Detection (DPD) message parameters for IKE v1 protocol.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

`[ no ] ikev1 keepalive dpd interval` *`interval`* **`timeout`** *`time`* **`num-retry`** *`retries`*

`no`

Deletes previously configured IPSec DPD Protocol settings.

`ikev1 keepalive dpd interval` *`interval`*

Specifies the time interval (in seconds) at which IPSec DPD Protocol messages are sent. *`interval`* is an integer from 10 through 3600.

`timeout` *`time`*

Specifies the amount of time (in seconds) allowed for receiving a response from the peer security gateway prior to re-sending the message. *`time`* is an integer from 10 through 3600.

`num-retry` *`retries`*

Specifies the maximum number of times that the system should attempt to reach the peer security gateway prior to considering it unreachable. *`retries`* is an integer from 1 through 100.

Usage

Use this command to configure the ISAKMP dead peer detection parameters in IKE v1 protocol. Tunnels belonging to crypto groups are perpetually kept “up” through the use of the IPSec Dead Peer Detection (DPD) packets exchanged with the peer security gateway.

Important: The peer security gateway must support RFC 3706 in order for this functionality to function properly.

This functionality is for use with the Redundant IPSec Tunnel Fail-over feature and to prevent IPSec tunnel state mismatches between the FA and HA when used in conjunction with Mobile IP applications. Regardless of the application, DPD must be supported/configured on both security peers. If the system is configured with DPD but it is communicating with a peer that does not have DPD configured, IPSec tunnels still come up. However, the only indication that the remote peer does not support DPD exists in the output of the **`show crypto isakmp security associations summary dpd`** command.

Important: If DPD is enabled while IPSec tunnels are up, it will not take affect until all of the tunnels are cleared.

Example

The following command configures IPSec DPD Protocol parameters to have an interval of *15*, a timeout of *10*, to retry each attempt *5* times:

```
ikev1 keepalive dpd interval 15 timeout 10 num-retry 5
```

ikev1 policy

Configures or creates an ISAKMP policy with the specified priority and enters ISAKMP Configuration Mode for IKE v1 protocol.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

[no] ikev1 policy *priority*

no

Removes a previously configured ISAKMP policy for IKE v1 protocol.

ikev1 policy *priority*

Specifies the priority of an ISAKMP policy as an integer from 0 through 100. ISAKMP policies for IKE v1 protocol with lower priority numbers take precedence over policies with higher priorities. “0” is the highest priority. Default: 0

Usage

Use this command to create ISAKMP policies to regulate how IPSec key negotiation is performed for IKE v1 protocol.
Internet Security Association Key Management Protocol (ISAKMP) policies are used to define Internet Key Exchange (IKE) SAs. The IKE SAs dictate the shared security parameters (i.e. which encryption parameters to use, how to authenticate the remote peer, etc.) between the system and a peer security gateway.
During Phase 1 of IPSec establishment, the system and a peer security gateway negotiate IKE SAs. These SAs are used to protect subsequent communications between the peers including the IPSec SA negotiation process.
Multiple ISAKMP policies can be configured in the same context and are used in an order determined by their priority number.

Example

Use the following command to create an ISAKMP policy with the priority *1* and enter the ISAKMP Configuration Mode:

```
ikev1 policy 1
```

ikev2-ikesa

Creates a new, or specifies an existing, IKEv2 security association transform set and enters the IKEv2 Security Association Configuration Mode.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

[no] ikev2-ikesa transform-set *name*

ikev2-ikesa transform-set *name*

Specifies the name of a new or existing security association transform set as an alphanumeric string of 1 through 127 characters.

Usage

Use this command to create a new or enter an existing IKEv2 security association transform-set. A list of up to four separate transform-sets can be created.
Entering this command results in the following prompt:

```
[context_name]hostname(cfg-ctx-ikev2ikesa-tran-set)#
```

IKEv2 Security Association Configuration Mode commands are defined in the *IKEv2 Security Association Configuration Mode Commands* chapter.

Example

The following command configures an IKEv2 security association transform set called *ikesa3* and enters the IKEv2 Security Association Configuration Mode:

```
ikev2-ikesa transform-set ikesa3
```

ims-auth-service

This command enables the creation, configuration or deletion of an IMS authorization service in the current context.

Product

GGSN, HA, IPSG, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

ims-auth-service *auth_svc_name* **[-noconfirm]**

{ no | default } ims-auth-service *auth_svc_name*

no

Deletes the specified IMS authorization service within the current context.

default

Restores default state of IMS authorization service, disabled for a specific context.

auth_svc_name

Specifies name of the IMS authorization service as a unique alphanumeric string of 1 through 63 characters. A maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to create/configure/delete an IMS authorization service for Gx interface support in the current context.
Entering this command results in the following prompt:
`[context_name]hostname(config-imsa-service)`
IMS authorization service configuration commands are described in the *IMS Authorization Service Configuration Mode Commands* chapter.

Example

The following command configures an IMS authorization service named *ims_interface1* within the current context:

```
ims-auth-service ims_interface1
```

ims-sh-service

Creates the specified IP Multimedia Subsystem (IMS) Sh service name to allow configuration of an Sh service.

Product

PDIF, SCM

Privilege

Administrator

Syntax

ims-sh-service *name*

no ims-sh-service *name*

no

Removes a previously configured IMS-Sh-service.

ims-sh-service *name*

Specifies the name of the IMS-Sh-service to be configured as an alphanumeric string of 1 through 63 characters.

Usage

The IMS-Sh-service is named in the pdif-service and/or cscf-service. Use this command to enter the IMS Sh Service Configuration Mode.
Entering this command results in the following prompt:
[*context_name*]*hostname*(config-ims-sh-service)#
IMS Sh Service Configuration Mode commands are defined in the *IMS Sh Service Configuration Mode Commands* chapter in this guide.

Example

The following example creates or enters an IMS Sh service named *ims-1*:

```
ims-sh-service ims-1
```

inspector

Configures a context-level inspector account within the current context.

Product

All

Privilege

Security Administrator

Syntax

inspector *user_name* **[encrypted] password** *password* **[ecs | noecs] [expiry-date** *date_time* **] [li-administration] [noecs] [timeout-absolute** *abs_seconds* **] [timeout-min-absolute** *abs_minutes* **] [timeout-idle** *timeout_duration* **] [timeout-min-idle** *idle_minutes* **]**

no inspector *user_name*

no

Removes a previously configured inspector account.

inspector *user_name*

Specifies a name for the context-level inspector account as an alphanumeric string of 1 through 32 characters.

[encrypted] password *password*

Specifies the password to use for the user which is being given context-level inspector privileges within the current context. The encrypted keyword indicates the password specified uses encryption.
password is an alphanumeric string of 1 through 63 characters without encryption, or 1 through 127 characters with encryption.
The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

ecs | noecs

Default: **noecs**
ecs: Permits the specific user to access ACS-specific configuration commands.
noecs: Prevents the specific user to access ACS-specific configuration commands.

expiry-date *date_time*

Specifies the date and time that this account expires. Enter the date and time in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.
Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

li-administration

Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

timeout-absolute *abs_seconds*

This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.
Specifies the maximum amount of time (in seconds) the context-level inspector may have a session active before the session is forcibly terminated. *abs_seconds* must be an integer from 0 through 300000000. The value 0 disables the absolute timeout. Default: 0

timeout-min-absolute *abs_minutes*

Specifies the maximum amount of time (in minutes) the context-level inspector may have a session active before the session is forcibly terminated. *abs_minutes* must be an integer from 0 through 525600 (365 days). The value 0 disables the absolute timeout. Default: 0

timeout-idle *timeout_duration*

This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.
Specifies the maximum amount of idle time (in seconds) the context-level inspector may have a session active before the session is terminated. *timeout_duration* must be an integer from 0 through 300000000. The value 0 disables the idle timeout. Default: 0

timeout-min-idle *idle_minutes*

Specifies the maximum amount of idle time (in minutes) the context-level inspector may have a session active before the session is terminated. *idle_minutes* must be an integer from 0 through 525600 (365 days). The value 0 disables the idle timeout. Default: 0

Usage

Create new context-level inspector or modify existing inspector's options, in particular, the timeout values. Inspector users have minimal read-only privileges. Refer to the *Command Line Interface Overview* chapter for more information.

Important: A maximum of 128 administrative users and/or subscribers may be locally configured per context.

Example

The following command creates a context-level inspector account named *user1*:

```
inspector user1 password secretPassword
```

The following command removes a context-level inspector account named *user1*:

```
no inspector user1
```

interface

Creates or deletes an interface or specifies an existing interface. By identifying an interface, the mode changes to configure this interface in the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

interface *name* **[broadcast | loopback | point-to-point | tunnel]**

no interface *name*

no

Indicates the interface specified is to be removed.

interface *name*

Specifies the name of the interface to configure. If *name* does not refer to an existing interface, the new interface is created if resources allow. *name* is an alphanumeric string of 1 through 79 characters.

broadcast

Creates an Ethernet broadcast (IP) interface and enters the Ethernet Configuration Mode. Default: Enabled

Important: Refer to the *Ethernet Interface Configuration Mode Command* chapter for more information.

loopback

Creates an internal IP address that is always UP, is not bound to any physical card/port, and can be reached by any interface configured in the current context. As a loopback interface uses all available physical ports, this type of interface is particularly useful for load-balancing. The interface must be configured for loopback when configuring Interchassis Session Recovery (ICSR). A total of 256 loopback interfaces can be configured. Default: Disabled
This loopback option is not used to setup a diagnostic test port so it should not be confused with the loopback option used in the various card/port configuration modes.

Important: Refer to the *Loopback Interface Configuration Mode Command* chapter for more information.

point-to-point

Creates a permanent virtual connection (PVC) in the current context and enters the PVC Configuration Mode. Currently, this type of interface is only used with an optical (ATM) line card.

Important: Refer to the *PVC Interface Configuration Mode Command* chapter for more information.

tunnel

Creates a tunnel interface to support the various tunnel interfaces. Currently only IPv6-over-IPv4 and GRE tunnel interfaces are supported.

Important: Refer to the *Tunnel Interface Configuration Mode Commands* chapter for more information.

Usage

Use this command to enter or create the interface configuration mode for an existing interface or for a newly defined interface. This command is also used to remove an existing interface when it longer is needed.

Important: If no keyword is specified, broadcast is assumed and the interface is Ethernet by default.

For IPv6-over-IPv4 or GRE tunneling, you need to specify the interface type as **tunnel**.

Example

The following command enters the Ethernet Interface Configuration Mode creating the interface *sampleService*, if necessary:

```
interface sampleInterface
```

The following command removes *sampleService* as being a defined interface:

```
no interface sampleInterface
```

The following command enters the Tunnel Interface Configuration Mode creating the interface *GRE_tunnel1*, if necessary:

```
interface GRE_tunnel1 tunnel
```

ip access-group

Configures an access group with an Access Control List (ACL) for IP traffic for the current context. The Context-level ACL is applied only to outgoing packets.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip access-group *name* **[in | out] [** *priority_value* **]**

no ip access-group *name* **[in | out]**

no

Indicates the specified ACL rule is to be removed from the group.

ip access-group *name*

Specifies the ACL rule to be added/removed from the group.
In Release 8.1 and later, *name* is an alphanumeric string of 1 through 47 characters.
In Release 8.0, *name* is an alphanumeric string of 1 through 79 characters.

Important: Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 256-rule limit for the context.

in | out

The **in** and **out** keywords are deprecated and are only present for backward compatibility. The Context-level ACL are applied only to outgoing packets.

priority_value

Specifies the priority of the access group. 0 is the highest priority. If *priority_value* is not specified, the priority is set to 0. *priority_value* must be an integer from 0 through 4294967295. Default: 0
If access groups in the list have the same priority, the last one entered is used first.

Usage

Use this command to add IP access lists (refer to the **ip access-list** command) configured with in the same context to an ACL group.
Refer to the *Access Control Lists* appendix of the *System Administration Guide* for more information on ACLs.

Example

The following commands add *sampleGroup* to the context-level ACL with a priority of *0*:

```
ip access-group sampleGroup 0
```

ip access-list

Enables creation, configuration or deletion of an IP Access List in the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip access-list *name*

{ default | no } ip access-list *name*

default

Sets the context's default access control list to that specified by *name*.

no

Removes the specified access list.

ip access-list *name*

Specifies the access list name.
In Release 8.0, *name* is an alphanumeric string of 1 through 79 characters.
In Release 8.1 and later, *name* is an alphanumeric string of 1 through 47 characters.
If the named access list does not exist, it is created, and the CLI mode changes to the ACL Configuration Mode, wherein the access list can be configured.
If the named access list already exists, the CLI mode changes to the ACL Configuration Mode, wherein the access list can be reconfigured.

Usage

Executing this command enters the ACL Configuration Mode in which rules and criteria are defined for the ACL.

Important: A maximum of 64 rules can be configured per ACL. The maximum number of ACLs that can be configured per context is limited by the amount of available memory in the VPN Manager software task; it is typically less then 200.

The no version of this command deletes the ACL.
Refer to the *Access Control Lists* appendix of the *System Administration Guide* for more information on ACLs.

Example

The following command creates an access list named *sampleList*, and enters the ACL Configuration Mode:

```
ip access-list sampleList
```

ip arp

Configures the allocation retention priority (ARP) options for the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip arp *ip_address mac_address* **[vrf** *vrf_name* **]**

no ip arp *ip_address mac_address*

no

Removes the ARP configuration data for the specified IP address from the configuration.

ip_address

Specifies the IP address for which to configure the ARP options where *ip_address* is an IP address expressed in IPv4 dotted-decimal notation.

mac_address

Specifies the media-specific access control layer address for the IP address. *mac_address* must be specified as a an 6-byte hexadecimal number with each byte separated by a colon, for example., “AA:12:bb:34:f5:0E”.

vrf *vrf_name*

Associates a Virtual Routing and Forwarding (VRF) context with this static ARP entry.
vrf_name is name of a preconfigured virtual routing and forwarding (VRF) context configured in *Context Configuration Mode* via the **ip vrf** command.

Usage

Manage the IP address mapping which is a logical/virtual identifier to the more lower layer addressing used for address resolution in ICMP messages.
For tunnel-based interface, network IP pool can have overlapping ip-addresses across Verve. To manage it adding a preconfigured VRF context is required to associate with an static ARP entry. By default, the ARP is added in the given context. If the VRF name is specified, then the ARP is added to the VRF ARP table.

Example

The following commands set the IP and MAC address for the current context then remove it from the configuration:

```
ip arp 10.2.3.4 F1:E2:D4:C5:B6:A7

no ip arp 10.2.3.4
```

The following commands set the IP and MAC address for a VRF context *vrf1* in the configuration:

```
ip arp 10.2.3.4 F1:E2:D4:C5:B6:A7 vrf vrf1
```

ip as-path access-list

Defines Border Gateway Protocol (BGP) Autonomous System (AS) Path access lists.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

ip as-path access-list *list_name* **[{ deny | permit }** *reg_expr* **]**

no ip as-path access-list *list_name* **[{ deny | permit }** *reg_expr* **]**

no

Remove the specified regular expression from the AS path access list.

ip as-path access-list *list_name*

Specifies the name of an AS path list as an alphanumeric string of 1 through 79 characters.

{ deny | permit }

deny: Denies access to AS paths that match the regular expression.
permit: Allows access to AS paths that match the regular expression.

reg_expr

A regular expression to define the AS paths to match. *reg_expr* is an alphanumeric string of 1 through 254 characters.

Important: The **?** (question mark) character is not supported in regular expressions for this command.

Usage

Use this command to define AS path access lists for the BGP router in the current context. The chassis supports a maximum of 64 access lists per context.

Example

The following command creates an AS access list named *ASlist1* and permits access to AS paths:

```
ip as-path access-list ASlist1 permit
```

ip dns-proxy source-address

Enables the proxy DNS functionality and identifies this context as the destination context for all redirected DNS requests.

Important: This command must be entered in the destination context for the subscriber. If there are multiple destination contexts for different subscribers, the command must be entered in each context.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

`[ no ] ip dns-proxy source-address` *`ip_address`*

`no`

Removes the address in this context as a destination for redirected DNS packets.

`ip dns-proxy source-address` *`ip_address`*

Specifies an interface in this context used for redirected DNS packets. *`ip_address`* must be entered using IPv4 dotted-decimal notation.

Usage

Use this command to identify the interface in this context where redirected DNS packets are sent to the home DNS. The system uses this address as the source address of the DNS packets when forwarding the intercepted DNS request to the home DNS server. For a more detailed explanation of the proxy DNS intercept feature, see the **`proxy-dns intercept-list`** command.

Example

The following command identifies an interface with an address of *`10.23.255.255`* in a destination context where the system forwards all intercepted DNS requests:

```
ip dns-proxy source-address 10.23.255.255
```

ip domain-lookup

Enables or disables domain name lookup via domain name servers for the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip domain-lookup

no ip domain-lookup

no

Disables domain name lookup.

ip domain-lookup

Enables domain name lookup.

Usage

Domain name look up is necessary if the subscribers configured for the context are to be allowed to use logical host names for services which requires the host name resolution via DNS.

Example

```
ip domain-lookup

no ip domain-lookup
```

ip domain-name

Configures or removes a logical domain name for the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip domain-name *name*

no ip domain-name *name*

no

Indicates the logical domain name for the current context is to be removed.

ip domain-name *name*

Specifies the logical domain name to use for domain name server address resolution. *name* is an alphanumeric string of 1 through 1023 characters formatted to be a valid IP domain name.

Usage

Set a logical domain name if the context is to be accessed by logical domain name in addition to direct IP address.

Example

```
ip domain-name sampleName.org
```

ip forward

Configures an IP forwarding policy to forward outgoing pool packets whose flow lookup fails to the default-gateway.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ip forward outbound unused-pool-dest-address default-gateway
```

no

Disables forwarding to the default gateway.

ip forward outbound unused-pool-dest-address default-gateway

Enables forwarding to the default gateway.

Usage

Use this command to set an IP forwarding policy that forwards outgoing pool packets whose flow lookup fails to the default gateway. By default, the behavior is to either send an ICMP Unreachable message or to discard the packet depending on the configuration of the IP pool.
Pool packets coming from the linecard whose flow lookup fails are discarded or ICMP unreachable is sent irrespective of whether this command is configured or not.

Example

To enable this functionality, enter the following command:

```
ip forward outbound unused-pool-dest-address default-gateway
```

To disable this functionality, enter the following command:

```
no ip forward outbound unused-pool-dest-address default-gateway
```

ip identification packet-size-threshold

Configures the packet size above which system will assign unique IP header identification.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

ip identification packet-size-threshold *size*

default ip identification packet-size-threshold

default

Restores default value of 576 bytes to IP packet size for fragmentation threshold.

ip identification packet-size-threshold *size*

Specifies the size of IP packet in bytes above which system will assign unique IP header identification for system generated IP encapsulation headers (such as MIP data tunnel). *size* is an integer from 0 through 2000. Default: 576

Usage

This configuration is used to set the upper limit of the IP packet size. All packets above that size limit will be considered “fragmentable”, and an unique non-zero identifier will be assigned.

Example

The following commands set the IP packet size to 1024 bytes as threshold. above this limit system will assign unique IP header identification for system generated IP encapsulation headers:

```
ip identification packet-size-threshold 1023
```

ip localhost

Configures or removes the static local host logical name to IP address mapping for the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip localhost *name ip_address*

no ip localhost *name ip_address*

no

Specifies that the static mapping must be removed.

ip localhost *name*

Specifies the logical host name (DNS) for the local machine on which the current context resides. *name* is an alphanumeric string of 1 through 1023 characters formatted to be a valid IP host name.

ip_address

Specifies the IP address for the static mapping. *ip_address* must be expressed in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Avoid excessive DNS lookups across the network by statically mapping the logical host name to the local host's context.

Example

```
ip localhost localHostName 10.2.3.4

no ip localhost localHostName 10.2.3.4
```

ip name-servers

Modifies the list of domain name servers the current context may use for logical host name resolution.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip name-servers *ip_address secondary_ip_address*

no ip name-servers *ip_address*

no

Indicates the name server specified is to be removed from the list of name servers for the current context.

ip name-servers *ip_address*

Specifies the IP address of a domain name server using IPv4 dotted-decimal or IPv6 colon-separated notation.

secondary_ip_address

Specifies the IP address of a secondary domain name server using either IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Manage the list of name servers the current context may use in resolving logical host names.
The DNS can be specified at the Context level in Context configuration as well as at the APN level in APN Configuration Mode with **dns** and **ipv6 dns** commands, or it can be received from AAA server.
When DNS is requested in PCO configuration, the following preference will be followed for DNS value:

1. DNS Values received from LNS have the first preference.
2. DNS values received from RADIUS Server has the second preference.
3. DNS values locally configured with APN with **dns** and **ipv6 dns** commands has the third preference.
4. DNS values configured at context level has the last preference.

Important: The same preference would be applicable for the NBNS servers to be negotiated via ICPC with the LNS.

Example

```
ip name-servers 10.2.3.4
```

ip pool

Enables creation, configuration or deletion of IP address pools in the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip pool *pool_name* **{** *ip_address subnet_mask* **|** *ip_address_mask_combo* **| range** *start_ip_address end_ip_address* **} [address-hold-timer** *address_hold_timer* **] [advertise-if-used] [alert-threshold [group-available | pool-free | pool-hold | pool-release | pool-used]** *low_thresh* **[clear** *high_thresh* **]] [explicit-route-advertise] [group-name** *group_name* **] [include-nw-bcast] [napt-users-per-ip-address** *users_per_ip* **[alert-threshold { { pool-free | pool-hold | pool-release | pool-used }** *low_thresh* **[clear** *high_thresh* **] } +] [max-chunks-per-user** *max_chunks_per_user* **[nat-binding-timer** *nat_binding_timer* **] [nexthop-forwarding-address** *ip_address* **] [on-demand] [port-chunk-size** *port_chunk_size* **] [port-chunk-threshold** *port_chunk_threshold* **] [send-nat-binding-update] +] [nat** *priority* **] [nat-one-to-one [alert-threshold { { pool-free | pool-hold | pool-release | pool-used }** *low_thresh* **[clear** *high_thresh* **] } +] [nat-binding-timer** *nat_binding_timer* **] [nexthop-forwarding-address** *ip_address* **] [on-demand] [send-nat-binding-update] +] [nat-realm users-per-nat-ip-address** *users* **[on-demand [address-hold-timer** *address_hold_timer* **]]] [nexthop-forwarding-address** *ip_address* **[overlap vlanid** *vlan_id* **] [respond-icmp-echo** *ip_address* **]] [nw-reachability server** *server_name* **] [policy allow-static-allocation] [private** *priority* **] [public** *priority* **] [resource** *priority* **] [send-icmp-dest-unreachable] [srp-activate] [static] [suppress-switchover-arps] [tag { none | pdif-setup-addr }] [unicast-gratuitous-arp-address** *ip_address* **]** [**vrf** *vrf_name* {[**mpls-label input** *in_label_value* | **output** *out_label_value1* [*out_label_value2*] }] +

no ip pool *pool_name* **[address-hold-timer] [advertise-if-used] [alert-threshold [[group-available] [pool-free] [pool-hold] [pool-release] [pool-used] +] [explicit-route-advertise] [group-name] [include-nw-bcast] [nexthop-forwarding-address [respond-icmp-echo]] [nw-reachability server] [policy allow-static-allocation] [send-icmp-dest-unreachable] [srp-activate] [suppress-switchover-arps] [tag { none | pdif-setup-addr }] [unicast-gratuitous-arp-address] + [send-nat-binding-update]**

no

Removes the specified IP address pool from the current context's configuration, or disables the specified option(s) for the specified IP pool.

no alert-threshold

This command without any optional keywords disables all alert thresholds.

ip pool *name*

Specifies the logical name of the IP address pool. *name* must be an alphanumeric string of 1 through 31 characters.

Important: An error message displays if the **ip** *pool name* and the *group name* in the configuration are the same. An error message displays if the **ip** *pool name* or *group name* are already used in the context.

ip_address

Specifies the beginning IP address of the IP address pool using IPv4 dotted-decimal.

subnet_mask

Specifies the IP address mask bits to determine the number of IP addresses in the pool. *ip_mask* must be specified using IPv4 dotted-decimal notation.
1 bits in the *ip_mask* indicate that bit position in the *ip_address* must also have a value of 1.
0 bits in the *ip_mask* indicate that bit position in the *ip_address* does not need to match – the bit can be either a 0 or a 1.
For example, if the IP address and mask are specified as *172.168.10.0* and *255.255.255.224*, respectively, the pool will contain IP addresses in the range *172.168.10.0* through *172.168.10.31* for a total of 32 addresses.

ip_address_mask_combo

Specifies a combined IP address subnet mask bits to indicate what IP addresses the route applies to. *ip_address_mask_combo* must be specified using CIDR notation where the IP address is specified using IPv4 dotted-decimal notation and the mask bits are a numeric value which is the number of bits in the subnet mask.

range *start_ip_address end_ip_address*

Specifies the IP addresses for the IP pool as a range of addresses.
start_ip_address specifies the beginning of the range of addresses for the IP pool.
end_ip_address specifies the end of the range of addresses for the IP pool.
The IP address range must be specified using IPv4 dotted-decimal notation.
For example, if *start_ip_address* is specified as *172.168.10.0* and *end_ip_address* is specified as *172.168.10.31* the IP pool will contain addresses in the range *172.168.10.0* through *172.168.10.31* for a total of 32 addresses.

private [*priority* **]**

Address pool may only be used by mobile stations which have requested an IP address from a specified pool. When private pools are part of an IP pool group, they are used in a priority order according to the precedence setting. *priority* must be an integer from 0 through 10 with 0 being the highest priority. The default value is 0.

public [*priority* **]**

Address pool is used in priority order for assigning IP addresses to mobile stations which have not requested a specific address pool. *priority* must be an integer from 0 through 10 with 0 being the highest priority. The default value is 0.

static

Address pool is used for statically assigned mobile stations. Statically assigned mobile stations are those with a fixed IP address at all times.

tag { none | pdif-setup-addr }

Default: **none**
none: default tag for all IP address pools
pdif-setup-addr: pool with this tag should only be used for PDIF calls.

address-hold-timer *seconds*

When this is enabled, and an active subscriber is disconnected, the IP address is held or considered still in use, and is not returned to the free state until the address-hold-timer expires. This enables subscribers who reconnect within the length of time specified (in seconds) to obtain the same IP address from the IP pool. *seconds* is the time in seconds and must be an integer from 0 through 31556926.

alert-threshold { group-available | pool-free | pool-hold | pool-release | pool-used } *low_thresh* **[clear** *high_thresh* **]**

Default: All thresholds are disabled.
Configures IP address pool-level utilization thresholds. These thresholds take precedence over context-level IP pool thresholds.
group-available: Set an alert based on the available percentage of IP addresses for the entire IP pool group.
pool-free: Set an alert based on the percentage of IP addresses that are unassigned in this IP pool.
pool-hold: Set an alert based on the percentage of IP addresses from this IP pool that are on hold.
pool-release: Set an alert based on the percentage of IP addresses from this IP pool that are in the release state.
pool-used: This command sets an alert based on the percentage of IP addresses that have been assigned from this IP pool.

Important: Refer to the **threshold available-ip-pool-group** and **threshold monitoring** commands in this chapter for additional information on IP pool utilization thresholding.

low_thresh: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer between 0 and 100.
clear *high_thresh*: The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. It may be configured as an integer between 0 and 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

group-name *group_name*

Assigns one or more preconfigured IP pools to the IP pool group. *group_name* is case sensitive and must be an alphanumeric string of 1 through 31 characters. One or more IP pool groups are assigned to a context and one IP pool group consists one or more IP pool(s).
IP pool group name is used in place of an IP pool name. When specifying a desired pool group in a configuration the IP pool with the highest precedence is used first. When that IP pool's addresses are exhausted the pool with the next highest precedence is used.

include-nw-bcast

Includes the network and broadcast addresses as part of the pool.

To remove the **include-nw-bcast** option from the ip pool, use the **no ip pool test include-nw-bcast** command.

napt-users-per-ip-address *users_per_ip* **[alert-threshold { { pool-free | pool-hold | pool-release | pool-used } *low_thresh* [clear *high_thresh*] } +] [max-chunks-per-user** *max_chunks_per_user* **[nat-binding-timer** *nat_binding_timer* **] [nexthop-forwarding-address** *ip_address* **] [on-demand] [port-chunk-size** *port_chunk_size* **] [port-chunk-threshold** *port_chunk_threshold* **] [send-nat-binding-update] +**

Important: In UMTS deployments this keyword is available in 9.0 and later releases. In CDMA deployments this keyword is available in 8.3 and later releases.

Important: In UMTS deployments, on upgrading from Release 8.1 to Release 9.0, and in CDMA deployments, on upgrading from Release 8.1 to 8.3, all NAT realms configured in Release 8.1 using the **nat-realm** keyword must be reconfigured using either the **nat-one-to-one** (for one-to-one NAT realms) or the **napt-users-per-ip-address** (for many-to-one NAT realms) keywords.

Configures many-to-one NAT realms.

- *users_per_ip*: Specifies how many users can share a single NAT IP address as an integer from 2 through 2016.
- **alert-threshold**: Specifies the alert threshold for the pool:

Important: Thresholds configured using the **alert-threshold** keyword are specific to the pool that they are configured in. Thresholds configured using the **threshold ip-pool-*** commands in the Context Configuration Mode apply to all IP pools in that context, and override the threshold configurations set within individual pools.

- **pool-free**: Percentage free alert threshold for this pool
- **pool-hold**: Percentage hold alert threshold for this pool
- **pool-release**: Percentage released alert threshold for this pool
- **pool-used**: Percentage used alert threshold for this pool
- *low_thresh*: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. *low_thresh* must be an integer from 0 through 100.
- **clear** *high_thresh*: The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. *high_thresh* must be an integer from 0 through 100.

Important: The *high_thresh* value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

- **max-chunks-per-user** *max_chunks_per_user*: Specifies the maximum number of port chunks to be allocated per subscriber in the many-to-one NAT pool. *max_chunks_per_user* must be an integer from 1 through 2016. Default: 1
- **nat-binding-timer** *binding_timer*: Specifies NAT Binding Timer for the NAT pool. *timer* must be an integer from 0 through 31556926. If set to 0, is disabled. Default: 0

- **nexthop-forwarding-address** *address*: Specifies the nexthop forwarding address for this pool. *address* must be an IPv4 or IPv6 address. If configured for a NAT pool, packets that are NATed using that NAT pool will be routed based on the configured nexthop address.

Important: The **nexthop-forwarding-address** support for NAT IP pools is functional only in later releases of Release 9.0 and in 10.0 and later releases.

- **on-demand**: Specifies allocating IP when matching data traffic begins.
- **port-chunk-size** *size*: Specifies NAT port chunk size (number of NAT ports per chunk) for many-to-one NAT pool. *size* must be an integer from 32 through 32256.

Important: The **port-chunk-size** configuration is only available for many-to-one NAT pools.

- **port-chunk-threshold** *chunk_threshold*: Specifies NAT port chunk threshold in percentage of number of chunks for many-to-one NAT pool. *chunk_threshold* must be an integer from 1 through 100. Default: 100%

Important: The **port-chunk-threshold** configuration is only available for many-to-one NAT pools.

- **send-nat-binding-update**: Specifies sending NAT binding updates to AAA for this realm. Default: Disabled

Important: **send-nat-binding-update** is not supported for many-to-one realms.

The following IP pool configuration keywords can also be used in the many-to-one NAT pool configuration:

- **group-name** *group_name*: Specifies the pool group name. The grouping enables to bind discontiguous IP address blocks in individual NAT IP pools to a single pool group.

  This keyword is available for NAT pool configuration only in Release 10.0 and later.

  NAT pool and NAT pool group names must be unique.

  group_name is an alphanumeric string of 1 through 31 characters that is case sensitive.

- **srp-activate**

  Activates the IP pool for Interchassis Session Recovery (ICSR).

nat *priority*

Designates the IP address pool as a Network Address Translation (NAT) address pool.
priority specifies the priority of the NAT pool. 0 is the highest priority. If *priority* is not specified, the priority is set to 0.
Must be a value from 0 (default) to 10.

Important: This functionality is currently supported for use with systems configured as an A-BG or P-CSCF.

nat-one-to-one [alert-threshold { { pool-free | pool-hold | pool-release | pool-used } *low_thresh* [clear *high_thresh*] } +] [nat-binding-timer

nat_binding_timer **] [nexthop-forwarding-address** *ip_address* **] [on-demand] [send-nat-binding-update] +**

Important: In UMTS deployments this keyword is available in Release 9.0 and later releases. In CDMA deployments this keyword is available in Release 8.3 and later releases.

Important: In UMTS deployments, on upgrading from Release 8.1 to Release 9.0, and in CDMA deployments, on upgrading from Release 8.1 to Release 8.3, all NAT realms configured in Release 8.1 using the **nat-realm** keyword must be reconfigured using either the **nat-one-to-one** (for one-to-one NAT realms) or the **napt-users-per-ip-address** (for many-to-one NAT realms) keywords.

Configures one-to-one NAT realm.

- **alert-threshold**: Specifies alert threshold for this pool:

Important: Thresholds configured using the **alert-threshold** keyword are specific to the pool in which they are configured. Thresholds configured using the **threshold ip-pool *** commands in the Context Configuration Mode apply to all IP pools in the context, and override the threshold configurations set within individual pools.

- **pool-free**: Percentage free alert threshold for this pool
- **pool-hold**: Percentage hold alert threshold for this pool
- **pool-release**: Percentage released alert threshold for this pool
- **pool-used**: Percentage used alert threshold for this pool
- *low_thresh*: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. *low_thresh* must be an integer from 0 through 100.
- **clear** *high_thresh*: The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. *high_thresh* must be an integer from 0 through 100.

Important: The *high_thresh* value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

- **nat-binding-timer** *nat_binding_timer*: Specifies NAT Binding Timer for the NAT pool. *binding_timer* must be an integer from 0 through 31556926. If set to 0, is disabled.

Important: For many-to-one NAT pools, the default NAT Binding Timer value is 60 seconds. For one-to-one NAT pools, it is 0. By default, the feature is disabled—the IP addresses/ port-chunks once allocated will never be freed.

- **nexthop-forwarding-address** *ip_address*: Specifies the nexthop forwarding address for this pool. *address* must be an IPv4 or IPv6 address. If configured for a NAT pool, packets that are NATed using that NAT pool will be routed based on the configured nexthop address.

Important: The **nexthop-forwarding-address** support for NAT IP pools is functional only in later releases of Release 9.0 and in Release 10.0 and later releases.

- **on-demand**: Specifies allocating IP address when matching data traffic begins.

- **send-nat-binding-update**: Specifies sending NAT binding updates to AAA for this realm. Default: Disabled

Important: **send-nat-binding-update** is not supported for many-to-one realms.

The following IP pool configuration keywords can also be used in the one-to-one NAT pool configurations:

- **address-hold-timer** *address_hold_timer*
- **group-name** *group_name*: Specifies the pool group name. The grouping enables to bind discontiguous IP address blocks in individual NAT IP pools to a single pool group. NAT pool and NAT pool group names must be unique. *group_name* is an alphanumeric string of 1 through 31 characters that is case sensitive. This keyword is available for NAT pool configuration only in StarOS 10.0 and later releases.
- **srp-activate**: Activates the IP pool for Interchassis Session Recovery (ICSR).

---

nat-realm users-per-nat-ip-address *users* **[on-demand [address-hold-timer** *address_hold_timer* **]]**

Important: The **nat-realm** keyword is only available in Release 8.1.

Important: In Release 8.1, the NAT On-demand feature is not supported.

Important: This functionality is currently supported for use with systems configured as an A-BG or P-CSCF.

Designates the IP address pool as a Network Address Translation (NAT) realm pool.
users-per-nat-ip-address *users*: Specifies the number of users sharing a single NAT IP address as an integer from 1 through 5000.
on-demand: Specifies to allocate IP when matching data traffic begins.
address-hold-timer *address_hold_timer*: Specifies the address hold timer (in seconds) for this pool as an integer from 0 through 31556926. If set to 0, the address hold timer is disabled.

---

nexthop-forwarding-address *ip_address*

A subscriber that is assigned an IP address from this pool is forwarded to the next hop gateway with the specified IP address.

---

overlap vlanid *vlan_id*

When a nexthop forwarding address is configured, this keyword can be configured to enable over-lapping IP address pool support and associates the pool with the specified virtual LAN (VLAN). *vlan_id* is the identification number of a VLAN assigned to a physical port and can be configured to any integer from 1 through 4095.
For more information on configuring VLANs, refer to the *System Administration Guide*.

Important: This functionality is currently supported for use with systems configured as an HA, or as a PDSN for Simple IP, or as a GGSN. This keyword can only be issued for pools of type private or static and must be associated with a different nexthop forwarding address and VLAN. A maximum of 256 over-lapping pools can be configured per context and a maximum of 256 over-lapping pools can be configured per HA or simple IP PDSN. For GGSNs, the total

number of pools is limited by the number of VLANs defined but the maximum number per context is 256. Additional network considerations and configuration outside of the system may be required.

nw-reachability server *server_name*

Binds the name of a configured network reachability server to the IP pool and enables network reachability detection for the IP pool. This takes precedence over any network reachability server settings in a subscriber configuration.
server_name: Specifies the name of a network reachable server that has been defined in the current context, expressed as an alphanumeric string of 1 through 16 characters.

Important: Also see the following commands for more information: Refer to the **policy nw-reachability-fail** command in the HA Configuration Mode to configure the action that should be taken when network reachability fails. Refer to the **nw-reachability server** command in this chapter to configure network reachability servers. Refer to the **nw-reachability-server** command in the Subscriber Configuration Mode to bind a network reachability server to a specific subscriber.

respond-icmp-echo *ip_address*

Pings the first IP address from overlapping IP address pools.

Important: In order for this functionality to work, all of the pools should contain an initial IP address that can be pinged.

resource

Specifies this IP pool as a resource pool. The IP addresses in resource pools may have IP addresses that also exist in other resource pools. IP addresses from a resource pool should not be used for IP connectivity within the system where the pool is defined. These IP addresses should be allocated for sessions which are L3 tunneled through the system (IP-in-IP or GRE). It is possible for resource pools in the same context to have overlapping addresses when the terminating network elements for the L3 tunnels are in different VPNs.
Default: Disabled
Also refer to the *Subscriber Configuration Mode Commands* chapter for a description of the **l3-to-l2-tunnel address-policy** command.

send-icmp-dest-unreachable

When enabled, this generates an ICMP destination unreachable PDU when the system receives a PDU destined for an unused address within the pool. Default: Disabled

explicit-route-advertise

When enabled, the output of **show ip pool verbose** includes the total number of explicit host routes.
Default: Enabled

srp-activate

Activates the IP pool for Interchassis Session Recovery (ICSR).

suppress-switchover-arp

Suppress corresponding gratuitous ARP generation when a line card switchover occurs. Default: Disabled

unicast-gratuitous-arp-address *ip_address*

Perform a unicast gratuitous ARP to the specified IP address rather than broadcast gratuitous ARP when gratuitous ARP generation is required. Default: Perform broadcast gratuitous ARP.

vrf *vrf_name* **{ [mpls-label input** *in_label_value* **\| output** *out_label_value1* **[** *out_label_value2* **] }**

Associates a preconfigured Virtual Routing and Forwarding (VRF) context instance with this IP pool and configures the other MPLS label parameters like values of In and Out labels.

Important: This command must be used with next-hop parameters.

vrf_name is name of a preconfigured virtual routing and forwarding (VRF) context configured in Context Configuration Mode through **ip vrf** command.

- *in_label_value* is the MPLS label that identifies the inbound traffic destined for this pool.
- The *out_label_value1* and *out_label_value2* identify the MPLS labels to be added to the outgoing packets sent for subscriber from this pool. Where *out_label_value1* is the inner output label and *out_label_value2* is the outer output label.

MPLS label values must be an integer from 16 through 1048575.
By default, the pools configured are bound to the default VRF unless specified with a VRF name.

Important: You cannot have overlapping pool addresses using the same VRF. Also you cannot have two pools using different VRFs but the same in-label irrespective of whether the pools are overlapping or not. The pool must be private or static pool in-order to be associated with a certain VRF. If the VRF with such a name is not configured, then the pool configuration would return an error prompting to add the VRF before configuring a pool.

policy allow-static-allocation

Configures static address allocation policy for dynamic IP pool. This keyword enables a dynamic IP pool to accept a static address for allocation.

Important: In static allocation scenario, the pool group name is returned by AAA in the attribute **SN1-IP-Pool-Name**, and the IP address to use will be returned in the **Framed-IP-Address** attribute.

+

Indicates that more than one of the previous keywords can be entered within a single command.

Usage

Define one or more pools of IP addresses for the context to use in assigning IPs to mobile stations. This command is also useful in resizing existing IP pools to expand or contract the number of addresses allocated. If you resize an IP pool, the change is effective immediately.
When using the **ip pool** command to resize an IP pool, the type must be specified since by default the command assumes the type as public. In other words, the CLI syntax to resize an IP pool is the same syntax used to create the pool. See examples below.

```
ip pool pool1 100.1.1.0/24 static
```

The syntax to resize that pool would be:

```
ip pool pool1 100.1.1.0/25 static
```

A pool which is deleted will be marked as such. No new IP addresses will be assigned from a deleted pool. Once all assigned IP addresses from a deleted pool have been released, the pool, and all associated resources, are freed.

Important: If an IP address pool is matched to a ISAKMP crypto map and is resized, removed, or added, the corresponding security association must be cleared in order for the change to take effect. Refer to the **clear crypto** command in the Exec mode for information on clearing security associations.

Over-lapping IP Pools: The system supports the configuration of over-lapping IP address pools within a particular context. Over-lapping pools are configured using either the resource or overlap keywords.
The **resource** keyword allows over-lapping addresses tunneled to different VPN end points.
The **overlap** keyword allows over-lapping addresses each associated with a specific virtual LAN (VLAN) configured for an egress port. It uses the VLAN ID and the nexthop address to determine how to forward subscriber traffic with addresses from the pool thus resolving any conflicts with overlapping addresses.
Note that if an overlapping IP Pool is bound to an IPSec Tunnel (refer to the **match ip pool** command in the *Crypto Group Configuration Mode* chapter), that tunnel carries the traffic ignoring the nexthop configuration. Therefore, the IPSec Tunnel takes precedence over the nexthop configuration. (Thus, one can configure the overlapping IP Pool with fake VLAN ID and nexthop and still be able to bind it to an IPSec Tunnel for successful operation.
The **overlap** keyword allows over-lapping addresses each associated with a specific VLAN can only be issued for pools of type private or static and must be associated with a different nexthop forwarding address and VLAN. A maximum of 128 over-lapping pools can be configured per context and a maximum of 256 over-lapping pools can be configured per system.

Important: Overlapping IP address functionality is currently supported for use with systems configured as an HA for Mobile IP, or as a PDSN for Simple IP, or as a GGSN. For deployments in which subscriber traffic is tunneled from the FA to the HA using IP-in-IP, a separate HA service must be configured for each over-lapping pool.

IP Pool Address Assignment Method: IP addresses can be dynamically assigned from a single pool or from a group of pools. The addresses are placed into a queue in each pool. An address is assigned from the head of the queue and, when released, returned to the end. This method is known as least recently used (LRU).
When a group of pools have the same priority, an algorithm is used to determine a probability for each pool based on the number of available addresses, then a pool is chosen based on the probability. This method, over time, allocates addresses evenly from the group of pools.

Important: Note that setting different priorities on each individual pool in a group can cause addresses in some pools to be used more frequently.

Important: In NAT IP pool configurations, the minimum number of public IP addresses that must be allocated to each NAT pool must be greater than or equal to the number of Session Managers (SessMgrs) available on the system. On the ASR 5000, it is >= 84 public IP addresses. This can be met by a range of 84 host addresses from a single Class C. The remaining space from the Class C can be used for other allocations.

Example

The following commands define a private IP address pool, a public IP address pool, and a static address pool, respectively.

```
ip pool samplePool1 1.2.3.0 255.255.255.0 private

ip pool samplePool2 1.3.0.0 255.255.0.0 public

ip pool samplePool3 1.4.5.0 255.255.255.0 static
```

The following command defines a private IP pool specified with a range of IP addresses. The pool has 101 addresses.

```
ip pool samplePool4 range 10.5.5.0 10.5.5.100 private
```

The following command sets the address hold timer on the pool to *60* minutes (*3600* seconds):

```
ip pool samplePool4 address-hold-timer 3600
```

The following command removes the IP address pool from the configuration:

```
no ip pool samplePool1
```

The following command creates a static IP pool:

```
ip pool pool1 100.1.1.0/24 static
```

The following command resizes the static IP pool created in the previous example:

```
ip pool pool1 100.1.1.0/25 static
```

ip prefix-list

Creates an IP prefix list for filtering routes.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

ip prefix-list name *list_name* **[seq** *seq_number* **] { deny | permit } { any |** *network_address*/*net_mask* **[ge** *ge_value* **] [le** *le_value* **]**

no ip prefix-list *list_name* **[seq** *seq_number* **] { deny | permit } { any |** *network_address*/*net_mask* **[ge** *ge_value* **] [le** *le_value* **]**

no

Delete the specified prefix-list entry.

name *list_name*

Specifies a name for the prefix list as an alphanumeric string of 1 through 79 characters.

seq *seq_number*

Assigns the specified sequence number to the prefix list entry as an integer from 1 through 4294967295.

deny

Specifies prefixes to deny.

permit

Specifies prefixes to permit.

any

Matches any prefix.

network_address/*net_mask* **[ge** *ge_value* **] [le** *le_value* **]**

Specifies the prefix to match.
network_address/*net_mask*: the IP address and the length, in bits, of the network mask that defines the prefix. The IP address and mask must be entered in IPv4 dotted-decimal notation. When neither **ge** (greater than or equal to) or **le** (less than or equal to) are specified an exact match is assumed.
ge *ge_value*: Specifies the minimum prefix length to match as an integer from 0 through 32. If only the ge value is specified, the range is from the ge value to 32. The ge value must be greater than *net_mask* and less than the le value.
le *le_value*: Specifies the maximum prefix length to match as an integer from 0 through 32. If only the le value is specified, the range is from the *net_mask* to the le value. The le value must be less than or equal to 32.
The following equation describes the conditions that ge and le values must satisfy:
net_mask **<** *ge_value* **<** *le_value* **<= 32**

Usage

Use this command to filter routes by their IP prefix.

Example

```
ip prefix-list name prelist10 seq 5 permit 192.168.100.0/8 ge 12 le 24
```

ip prefix-list sequence-number

Enables or disables the inclusion of IP prefix list sequence numbers in the configuration file. This option is enabled by default.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ip prefix-list sequence-number
```

no

Disables the listing of IP prefix list sequence numbers in the configuration file.

ip prefix-list sequence-number

Enables the listing IP of prefix list sequence numbers in the configuration file.

Usage

Use this command to enable and disable the inclusion of IP prefix list sequence numbers in the configuration file.

Example

To disable the inclusion of IP prefix list sequence numbers in the configuration file, enter the following command:

```
no ip prefix-list sequence-number
```

ip route

Adds or removes routing information from the current context's configuration.

Product

All

Privilege

Administrator

Syntax

[no] ip route (*ip_address* | static bfd }

[no] ip route { *ip_address*/*ip_mask* | *ip_address ip_mask* } { *gateway_ip_address* | next-hop *next_hop_ip_address* | point-to-point | tunnel } *egress_intrfc_name* [cost *cost*] [precedence *precedence*][vrf *vrf_name*] +

[no] ip route static bfd *if-name gateway_ip_address*

---

no

Indicates the route specified by this options is to be removed from the configuration.

---

ip route *ip_address*/*ip_mask* | *ip_address ip_mask*

Specifies a destination IP address or group of addresses that will use this route.
ip_address/*ip_mask*: Specifies a combined IP address subnet mask bits to indicate what IP addresses to which the route applies. *ip_address* must be entered using IPv4 dotted-decimal or IPv6 colon-separated notation. *ip_mask*/ is entered using CIDR notation; the mask bits are a numeric value which is the number of bits in the subnet mask.
ip_address ip_mask: Specifies an IP address and the networking (subnet) mask pair which is used to identify the set of IP addresses to which the route applies. *ip_address* must be specified using the standard IPv4 dotted decimal notation. *ip_mask* must be specified using the standard IPv4 dotted decimal notation as network mask for subnets.
The mask as specified by *ip_mask* or resulting from *ip_address*/*ip_mask* is used to determine the network for packet routing.
0's in the resulting mask indicate the corresponding bit in the IP address is not significant in determining the network for packet routing.
1's in the resulting mask indicate the corresponding bit in the IP address is significant in determining the network.

---

gateway_ip_address **| next-hop** *next_hop_ip_address* **| point-to-point | tunnel**

Specifies which device or network to use when forwarding packets.
gateway_ip_address: Specifies the IP address of the network gateway to which to forward packets. The address must be entered in IPv4 dotted-decimal notation (###.###.###.###).
next-hop *next_hop_ip_address*: Specifies the next-hop IP address to which packets are to be forwarded. The address must be entered in IPv4 dotted-decimal notation.
point-to-point: Specifies that the egress port is an ATM point-to-point interface.
tunnel: Sets the static route for this egress interface as tunnel type, such as IPv6-over-IPv4 or GRE.

egress_intrfc_name

Specifies the name of the egress (out-bound) interface name in the current context as an alphanumeric string of 1 through 79 characters.

cost *cost*

Specifies the relative cost of the route. *cost* must be an integer from 0 through 255 where 255 is the most expensive. Default: 0

precedence *precedence*

Specifies the selection order precedence for this routing information. *precedence* must be an integer from 1 through 254 where 1 is the highest precedence. Default: 1

vrf *vrf_name*

Associates a Virtual Routing and Forwarding (VRF) context with this static route configuration. *vrf_name* is the name of a preconfigured VRF context configured in *Context Configuration Mode* via the **ip vrf** command.

ip route static bfd*if-name gateway_ip_address*

Creates a static IP route that will be associated with Bidirectional Forwarding Detection (BFD). For additional information, see the *BFD Configuration Mode Commands* chapter.
if-name: Specifies the interface Name of the Interface to which the static BFD neighbor is bound as an alphanumeric string of 1 through 79 characters.
gateway_ip_address : Specifies the gateway address of the BFD neighbor in IPv4 dotted-decimal notation.

Usage

Use this command to configure IP route parameters. Precedence and cost options tailor the route selections such that routes of the same precedence are grouped together then lowest cost is selected first. This results in route's being selected first by lower precedence then the cost is used if multiple route's are defined with the same precedence.
This command also configures static IP routes when implementing Bidirectional Forwarding Detection (BFD).

Important: A maximum of 1,200 static routes may be configured per context.

Virtual Routing and Forwarding (VRF) context can be associated with static IP route for BGP/MPLS, GRE, or IPSec tunnel support.

Example

The following command adds a route using the combined IP address and subnet mask form:

```
ip route 10.2.3.0/32 192.168.1.2 egressSample1 precedence 160
```

The following configures route options for a route specified using the distinct IP address and subnet mask form:

```
ip route 10.2.3.4 255.224.0.0 10.1.2.3 egressSample2 cost 43
```

The following deletes the two routes configured above:

```
no ip route 10.2.3.0/32 192.168.1.2 egressSample1 precedence 160

no ip route 10.2.3.4 255.224.0.0 10.1.2.3 egressSample2 cost 43
```

The following command adds a route using the combined IP address and subnet mask form and specifies the egress interface as tunnel type:

```
ip route 10.2.3.0/32 tunnel egressSample1 precedence 160 vrf vrf1
```

ip routing maximum-paths

Enables Equal Cost Multiple Path (ECMP) routing support and specifies the maximum number of ECMP paths that can be submitted by a routing protocol in the current context.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

ip routing maximum-paths [*max_num*]

[default | no] ip routing maximum-paths

default

Resets the command to its default setting of 4.

no

Disables ECMP for the current context.

ip routing maximum-paths *max_num*

The maximum number of ECMP paths that can be submitted by a routing protocol. *max_num* must be an integer from 1 through 10. Default: 4

Usage

Use this command to enable ECMP for routing and set the maximum number of ECMP paths that can be submitted by a routing protocol.

Example

To enable ECMP and set the maximum number of paths that may be submitted by a routing protocol in the current context to *10*, enter the following command:

```
ip routing maximum-paths 10
```

To disable ECMP in the current context, enter the following command:

```
no ip routing maximum-paths
```

ip routing overlap-pool

Configures the routing behavior for overlap-pool addresses.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] ip routing overlap-pool
```

default

Resets the command to its default setting of disabled.

no

Disables the routing behavior for overlap-pool addresses for the current context.

ip routing overlap-pool

Advertises overlap-pool addresses in dynamic routing protocols when overlap pools are configured using vlan-ids. Default: disabled

Usage

Use this command configuration to advertise overlap-pool addresses in dynamic routing protocols when overlap pools are configured using vlan-ids. If the “ip routing overlap-pool” is configured, then the overlap-addresses are added as interface addresses and advertised.

ip vrf

Creates a Virtual Routing and Forwarding (VRF) context instance, assigns a VTF id, and configures the VRF parameters for BGP/MPLS VPN, GRE tunnel, and IPSec interface configuration.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip vrf *vrf_name*

no ip vrf

no

Disables IP Virtual Routing and Forwarding (VRF) parameters.

ip vrf *vrf_name*

Specifies the name of the virtual routing and forwarding interface as an alphanumeric string of 1 through 79 characters.

\

Usage

Use this command to create a VRF context and assigns a VRF id for BGP/MPLS VPN, IPSec, GRE tunnel configuration in this context instance. This command used when system works as a BGP router with MPLS VPN and binds a MPLS VPN to system or to facilitate GRE or IPSec tunnelling. The addresses that assigned to this interface are visible in the VRF routing table.
This command switches the command mode to IP VRF Context Configuration Mode and changes the CLI prompt to:

```
[context_name>]host_name(config-context-vrf)#
```

If required, this command creates IP VRF Context Configuration Mode instance.
While using this command user must take note of the following:

- A VRF context instance must be created and configured before referring, associating, or binding the same with any command or mode.
- If interface binding to a VRF context instance is changed or any IP address assigned to the interface is deleted a warning will be displayed.
- All interface bound with a VRF context instance will be deleted when that VRF is removed/deleted.
- An interface can be bound to only one VRF context instance.
- A maximum of 100 VRF context instances can be configured on a system.

Refer to the *IP VRF Context Configuration Mode Commands* chapter for parameter configuration.

Example

The following command configures the virtual routing and forwarding context instance *vrf1* in a context:

```
ip vrf vrf1
```

ipms

Enables/disables/manages an intelligent packet monitoring system (IPMS) client service and enters the IPMS Client Configuration Mode within the current context.

Product

IPMS

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ipms [ -noconfirm ]
```

no

Deletes a previously configured IPMS client service.

ipms

Configures IPMS client service.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

WARNING: If this keyword option is used with **no ipms** command the IPMS client service will be deleted with all active/inactive IPMS sessions without prompting any warning or confirmation.

Usage

Use this command to enable/disable/manage the IPMS client service within a context and configure certain functionality. This command enables and allows the configuration of service enabling the system to function as an IPMS-enabled Access Gateway in a network. This command is also used to remove previously configured IPMS client service.
A maximum of 1 IPMS client can be configured per system.

Important: The IPMS is a license enabled external application support. Refer to the *IPMS Installation and Administration Guide* for more information on this product.

Refer to the *IPMS Installation and Administration Guide* and *IPMS Configuration Mode* chapter of this reference for additional information.

Example

The following command creates an IPMS client service name within the context:

```
ipms
```

ipsec

Creates a new or specifies an existing IPSec transform set and enters the IPSec Transform Set Configuration Mode for the current context.

Product

PDIF, SCM

Privilege

Security Administrator, Administrator

Syntax

[no] ipsec transform-set *name*

ipsec transform-set *name*

Specifies the name of a new or existing transform set as an alphanumeric string of 1 through 127 characters.

Usage

Use this command to create an new or enter an existing IPSec transform-set. Up to four transform-sets can be created.
Entering this command results in the following prompt:
[*context_name*]*hostname*(cfg-ctx-ipsec-tran-set)#
IPSec Transform Set Configuration Mode commands are defined in the *IPSec Transform Set Configuration Mode Commands* chapter.

Example

The following command configures an IPSec transform set called *ipsec12* and enters the IPSec Transform Set Configuration Mode:

```
ipsec transfrom-set ipsec12
```

ipsg-service

Creates an IP Services Gateway service, or specifies an existing IPSG service, in the current context and enters the IPSG RADIUS Snoop or IPSG RADIUS Server Configuration Mode.

Product

IPSG

Privilege

Security Administrator, Administrator

Syntax

ipsg-service *ipsg_service_name* **[mode { radius-server | radius-snoop }] [-noconfirm]**

no ipsg-service *ipsg_service_name* **[mode { radius-server | radius-snoop }]**

no

Deletes the named IPSG service.

ipsg-service *ipsg_service_name*

Specifies the name of the IPSG service to be configured. If *ipsg_service_name* does not refer to an existing service, the new service is created if resources allow.
ipsg_service_name is an alphanumeric string of 1 through 63 characters.

mode { radius-server | radius-snoop }

Configures the IPSG to perform as either a RADIUS server or as a device to extract user information from RADIUS accounting request messages (snoop). If the optional keyword **mode** is not entered, the system defaults to **radius-server**.

- **radius-server**: Creates an IP Services Gateway RADIUS Server service in the context and enters the IPSG RADIUS Server Configuration Mode.
- **radius-snoop**: Creates an IP Services Gateway RADIUS Snoop service in the context and enters the IPSG RADIUS Snoop Configuration Mode.

-noconfirm

Executes the command without an additional prompt and confirmation from the user.

Usage

Enter the IPSG RADIUS Snoop or IPSG RADIUS Server Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of one IPSG service can be configured per context.
Entering this command results in the following prompt (RADIUS Server shown):
[*context_name-service_name*]*hostname*(config-radius-server)#
IPSG service commands are defined in the *IPSG RADIUS Snoop Configuration Mode Commands* chapter or the *IPSG RADIUS Server Configuration Mode Commands* chapters.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: A large number of services greatly increases the complexity of system management and may impact overall system performance (i.e., resulting from system handoffs). Do not configure a large number of services unless your application requires it. Contact your Cisco service representative for more information.

Important: IP Services Gateway functionality is a license-controlled feature. A valid feature license must be installed prior to configuring an IPSG service. If you have not previously purchased this feature, contact your sales representative for more information.

For more information about the IP Services Gateway, refer to the *IP Services Gateway Administration Guide*.

Example

The following command configures an IPSG RADIUS Snoop service named *ipsg1* and enters the IPSG RADIUS Snoop Configuration Mode:

```
ipsg-service ipsg1 mode radius-snoop
```

ipv6 access-group

Configures the IPv6 Access group.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

ipv6 access-group *group name* **{** *priority_value* **}**

ipv6 access-group *group_name*

Specifies the name of the access group as an alphanumeric string of 1 through 79 characters.

priority_value

Specifies the priority of the access group. 0 is the highest priority. If *priority_value* is not specified the priority is set to 0. *priority_value* must be an integer from 0 through 4294967295. Default: 0
If access groups in the list have the same priority, the last one entered is used first.

Usage

Use this command to specify IPv6 access group name and priority. Use a lower value to indicate a higher priority for the group.

Example

```
ipv6 access-group group_1
```

ipv6 access-list

Configures access list (or packet filter) name and enters the IPv6 ACL Configuration Mode.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

[no] ipv6 access-list *name*

no

Indicates the access list specified is to be removed from the configuration.

ipv6 access-list *name*

Specifies the access list for which to enter the IPv6 ACL Configuration Mode or the list to remove. *name* is an alphanumeric string of1 through 79 characters.

Usage

Executing this command enters the IPv6 ACL Configuration Mode in which rules and criteria are defined for the ACL.

Example

```
ipv6 access-list samplelist

no ipv6 access-list samplelist
```

ipv6 dns-proxy

Configures the domain name server proxy for the context.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

ipv6 dns-proxy source-ipv4-address *ip_address*

no ipv6 dns-proxy source-ipv4-address *ip_address*

no

Removes the predefined IP address for local interface in the destination context.

ipv6 dns-proxy source-ipv4-address

Enables the IPv6 proxy DNS functionality for a context. PDSN will use this address as the source address of the IPv4 packets. Default: no address is configured.

ip_address

Specifies the IPv4 address of one of the local interface in the destination context to configure the IPv6 DNS proxy where *ip_address* must be specified using IPv4 dotted-decimal notation.

Usage

The IPv6 DNS proxy source IPv4 address is used as the source IP address for the DNS proxy transaction.

Example

The following command provides an example of configuring a IPv6 DNS proxy of *192.168.23.1*:

```
ipv6 dns-proxy source-ipv4-address 192.168.23.1
```

ipv6 neighbor

Adds a static IPv6 neighbor entry into the neighbor discovery table.

Product

PDIF

Privilege

Administrator, Security Administrator

Syntax

[no] ipv6 neighbor *ipv6_address hardware_address*

no

Removes the specified address.

ipv6 neighbor *ipv6_address hardware_address*

ipv6_address is the IP address of node to be added to the table.
hardware_address is the associated 48-bit MAC address.

Usage

Add a static IPv6 neighbor entry into the neighbor discovery table.

Example

Add the ipv6 address *fe80::210:83ff:fef7:7a9d::/24* and associated 48 bit MAC address *0:10:83:f7:7a:9d* to the table.

```
ipv6 neighbor fe80::210:83ff:fef7:7a9d::/24 0:10:83:f7:7a:9d
```

ipv6 pool

Modifies the current context's IP address pools by adding, updating or deleting a pool. This command also resizes an existing IP pool.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ipv6 pool *name* **{ 6to4 local-endpoint** *ipv4_address* **[default-relay-router** *router_address* **] | alert threshold | group-name** *name* **| policy { allow-static-allocation | dup-addr-detection} | prefix** *ip_address/len* **[6to4-tunnel local-endpoint** *ip_address* **| default-relay-router** *router_address* **] | range** *start_address end_address* **| suppress-switchover-arps } [private** *priority* **] [public** *priority* **] [shared** *priority* **] [static** *priority* **] [group-name** *name* **]**

no ipv6 pool *name*

---

no

Deletes the previously configured IPv6 pool.

---

ipv6 pool *name*

Specifies the logical name of the IP address pool as an alphanumeric string of 1 through 31 characters.

6to4-tunnel local-endpoint *ip_address*

Specifies the IPv4 address of the local interface to be used for IPv6-to-IPv4 compatible pool address construction.

---

alert threshold { 6to4 local-endpoint *ipv4_address* **| alert threshold | group-available | group-name** *name* **| policy { allow-static-allocation | dup-addr-detection } | pool-free | pool-used | prefix | range** *start_address end_address* **}**

Default: All thresholds are disabled.
Configures IP address pool-level utilization thresholds. These thresholds take precedence over context-level IPv6 pool thresholds.

- **6to4**: Sets an alert based on the IPv6 Pool for an IPv6-to-IPv4 compatible address type.
- **alert-threshold**: Sets an alert based on the percentage free alert threshold for this group.
- **group-available**: Sets an alert based on the percentage free alert threshold for this group.
- **group-name**: Sets an alert based on the IPv6 Pool Group.
- **policy allow-static-allocation**: Sets an alert based on the address allocation policy.
- **pool-free**: Sets an alert based on the percentage free alert threshold for this pool.
- **pool-used**: Sets an alert based on the percentage used alert threshold for this pool.
- **prefix**: Sets an alert based on the IPv6 Pool address prefix.
- **range**: Sets an alert based on the IPv6 address pool range of addresses.

- **suppress-switchover-arps**: Sets an alert based on the Suppress Gratuitous ARPs when performing a line card switchover.

---

group name *name*

IPv6 Pool Group.
The following options are available:

- **6to4**: IPv6 Pool for IPv6-to-IPv4 compatible address type
- **alert-threshold**: Percentage free alert threshold for this group
- **group-name**: IPv6 Pool Group
- **policy**: Configure an address allocation policy
- **prefix**: IPv6 Pool address prefix
- **range**: Configures IPv6 address pool to use a range of addresses
- **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card switchover

---

ipv4_address

Specifies the beginning IPv4 address of the IPv4 address pool. *ipv4_address* must be specified using IPv4 dotted-decimal notation.

---

default-relay-router *router address*

Specifies the default relay router for the tunnel.

---

policy allow-static-allocation

Allows a dynamic pool to accept a static address allocation.
The following options are available:

- **6to4**: IPv6 Pool for IPv6- to-IPv4 compatible address type
- **alert-threshold**: Percentage free alert threshold for this group
- **group-name**: IPv6 Pool Group
- **policy**: Configure an address allocation policy
- **prefix**: IPv6 Pool address prefix
- **range**: Configures IPv6 address pool to use a range of addresses
- **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card switchover

---

policy dup-addr-detection

This command is valid for IPv6 shared pools only (Sample syntax: **ipv6 pool** *name* **prefix** *ip_address/len* **shared policy dup-addr-detection**). When this policy is enabled, the IPv6 shared pool allows a prefix to be shared in different call sessions with different interface IDs for an IPv6 address. This allows the tracking of interface IDs per prefix and the detection of duplicated IDs.
With this policy disabled, the IPv6 shared pool will allow a prefix to be shared across different call sessions. The interface ID is not considered for any duplicate address detection. Default: Disabled
The following options are available:

- **6to4**: IPv6 pool for IPv6-to-IPv4 compatible address type
- **alert-threshold**: Percentage free alert threshold for this group
- **group-name**: IPv6 pool group

- **policy**: Configure an address allocation policy
- **prefix**: IPv6 pool address prefix
- **range**: Configures IPv6 address pool to use a range of addresses
- **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card switchover

---

prefix *ip_address/len*

Specifies the beginning IPv6 address of the IPv6 address pool. *ip_address/len* must be specified using IPv6 colon-separated with CIDR notation.

---

range *start_address end_address*

Configures an IPv6 address pool to use a range of addresses.
start_address specifies the beginning of the range of addresses for the IPv6 pool. It must be specified using IPv6 colon-separated notation.
end_address specifies the end of the range of addresses for the IPv6 pool. It must be specified using IPv6 colon-separated notation.

---

suppress-switchover-arps

Suppresses gratuitous ARPs when performing a line card switchover.
The following options are available:

- **6to4**: IPv6 Pool for IPv6-to-IPv4 compatible address type
- **alert-threshold**: Percentage free alert threshold for this group
- **group-name**: IPv6 Pool Group
- **policy**: Configure an address allocation policy
- **prefix**: IPv6 Pool address prefix
- **range**: Configures IPv6 address pool to use a range of addresses
- **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card switchover

---

private *priority* **| public** *priority* **| shared** *priority* **| static** *priority*

Default: **public**
private *priority*: Specifies that the address pool may only be used by mobile stations which have requested an IP address from a specified pool. When private pools are part of an IP pool group, they are used in a priority order according to the precedence setting. *priority* must be an integer from 0 through 10 with 0 being the highest. The default is 0.
public *priority*: Specifies that the address pool is used in priority order for assigning IP addresses to mobile stations which have not requested a specific address pool. *priority* must be n integer from 0 through 10 with 0 being the highest and with a default of 0.
shared *priority*: Specifies that the address pool that may be used by more than one session at any time. *priority* must be an integer from 0 through 10 with 0 being the highest and with a default of 0.
static *priority*: Specifies that the address pool is used for statically assigned mobile stations. Statically assigned mobile stations are those with a fixed IP address at all times. *priority* must be an integer from 0 through 10 with 0 being the highest and with a default of 0.

---

group-name *name*

Groups the IPv6 pools in to different groups. The subscribers/domain can be configured with the group-name instead of the prefix-pool names. *name* is the name of the group by which the IPv6 pool is to be configured expressed as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to modify the current context's IP address pools by adding, updating, or deleting a pool. Also use this command to resize an existing IP pool.

Example

The following command adds an IPv6 pool named *ip6Star*:

```
ipv6 pool ip6Star
```

ipv6 route

Configures a static IPv6 route to the next-hop router.

Product

All

Privilege

Administrator

Syntax

[no] ipv6 route *ipv6_address/prefix_length* **{ interface** *name* **| next-hop** *ipv6_address* **interface** *name* **} [cost** *cost* **] [precedence** *precedence* **]**

no

Removes the specified static route.

ipv6 route *ipv6_address/prefix_length*

Specifies a destination IPv6 address or group of addresses that will use this route. *ipv6_address/prefix_length* must be specified using IPv6 colon-separated with CIDR notation.

interface *name*

Specifies the name of the interface on this system associated with the specified route or next-hop address. *name* must be an existing interface name on the system expressed as an alphanumeric string of 1 through 79 characters.

next-hop *ipv6_address*

The IPv6 address of the directly connected next hop device in IPv6 colon-separated notation.

cost *cost*

Defines the number of hops to the next gateway as an integer from 0 through 255. Default: 0

precedence *precedence*

Indicates the administrative preference of the route. A low precedence specifies that this route takes preference over the route with a higher precedence. *precedence* must be an integer from 1 through 254. Default: 1

Usage

Use this command to create a static route and send data traffic to a next-hop device.

Example

T the following example configures a static route with IPv6 prefix/length *2001:0db8:3c4d:0015:0000:0000:abcd:ef12/24* to the next hop interface *egress1*:

```
ipv6 route 2001:0db8:3c4d:0015:0000:0000:abcd:ef12/24 interface egress1
```

isakmp disable-phase1-rekey

This command is deprecated. Use **ikev1 disable-phase1-rekey** command to configure the parameters for Phase1 SA rekeying when ISAKMP lifetime expires for IKE v1 protocol.

isakmp keepalive

This command is deprecated. Use **ikev1 keepalive dpd** command to configure ISAKMP IPSec Dead Peer Detection (DPD) message parameters for IKE v1 protocol.

isakmp policy

This command is deprecated. Use **ikev1 policy** command to create/configure an ISAKMP policy with the specified priority for IKE v1 protocol.

iups-service

Creates an Iu-PS service instance and enters the Iu-PS Service Configuration Mode. This mode defines the configuration and usage of Iu-PS interfaces between the SGSN and the RNCs in the UMTS radio access network (UTRAN). It defines both the control plane (GTP-C) and the data plane (GTP-U) between these nodes.

Important: For details about the commands and parameters for this mode, check the *IuPS Service Configuration Mode Commands* chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

iups-service *srvc_name*

no iups-service *srvc_name*

no

Remove the configuration for the specified Iu-PS service from the configuration for the current context.

iups-service *srvc_name*

Specifies the IuPS service name as a unique alphanumeric string of 1 through 63 characters.

Usage

Use this command to create, edit, or remove an Iu-PS service. Add up to eight definitions to be used with a single SGSN service so the SGSN can support multiple PLMNs.

Example

The following command creates an Iu-PS service named *iu-ps1*:

```
iups-service iu-ps1
```

The following command removes the Iu-PS service named *iu-ps1*:

```
no iups-service iu-ps1
```

l2tp peer-dead-time

Configures a delay when attempting to tunnel to a specific peer which is initially unreachable due to reasons such as a network issue or temporarily having reached its capacity.

Product

All

Privilege

Security Administrator, Administrator

Syntax

l2tp peer-dead-time *seconds*

default l2tp peer-dead-time

default

Rests the command to its default setting of 60.

peer-dead-time *seconds*

Specifies the interval (in seconds) to wait before attempting to tunnel to a specific peer which is initially unreachable as an integer from 5 through 64,000. Default: 60

Usage

The time to wait before trying to establish a tunnel to a known peer after the initial attempt was unsuccessful.

Example

The following example configures the delay in attempting to tunnel to a temporarily unreachable peer. The delay is set to *120* seconds in this example.

```
l2tp peer-dead-time 120
```

lac-service

Enters the LAC Service Configuration Mode, or is used to add or remove a specified L2TP Access Concentrator (LAC) service.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] lac-service *name*

no

Removes the specified lac-service from the current context.

lac-service *name*

Specifies the name of a LAC service to configure, add, or remove as an alphanumeric string of 1 through 63 characters that is case-sensitive.

Usage

Enter the LAC Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

To add a new LAC service named *LAC1* and enter the LAC Service Configuration Mode, enter the following command:

```
lac-service LAC1
```

To configure an existing LAC service named *LAC2*, enter the following command:

```
lac-service LAC2
```

To delete an existing LAC service named *LAC3*, enter the following command:

```
no lac-service LAC3
```

lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

lawful-intercept dictionary

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

lma-service

Creates an Local Mobility Anchor (LMA) service or specifies an existing LMA service and enters the LMA Service Configuration Mode for the current context.

Product

P-GW

Privilege

Administrator

Syntax

lma-service *service_name* **[-noconfirm]**

no lma-service *service_name*

lma-service *service_name*

Specifies the name of the LMA service. If *service_name* does not refer to an existing service, the new service is created if resources allow.
service_name is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no lma-service *service_name*

Removes the specified LMA service from the context.

Usage

Enter the LMA Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-lma-service)#
```

LMA Service Configuration Mode commands are defined in the *LMA Service Configuration Mode Commands* chapter.
Use this command when configuring the following eHRPD and PMIP SAE components: P-GW.

Example

The following command enters the existing LMA Service Configuration Mode (or creates it if it does not already exist) for the service named *lma-service1*:

```
lma-service lma-service1
```

The following command will remove *lma-service1* from the system:

```
no lma-service lma-service1
```

Ins-service

Enters the LNS Service Configuration Mode, or is used to add or remove a specified L2TP Network Server (LNS) service.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] lns-service *name*

no

Removes the specified lac-service from the current context.

lns-service *name*

Specifies the name of a LNS service to configure, add or remove as an alphanumeric string of 1 through 63 characters that is case-sensitive.

Usage

Enter the LNS Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

To add a new LNS service named *LNS1* and enter the LNS Service Configuration Mode, enter the following commands:

```
lns-service LNS1
```

To configure an existing LNS service named *LNS2*, enter the following command:

```
lns-service LNS2
```

To delete an existing LNS service named *LNS3*, enter the following command:

```
no lns-service LNS3
```

logging

Modifies the logging options for a specified system log server for the current context.

Product

All

Privilege

Administrator

Syntax

[no] logging syslog *ip_address* **[event-verbosity { min | concise | full }] [facility** *facilities* **] [pdu-data { none | hex | hex-ascii }] [pdu-verbosity** *pdu_level* **] [rate** *value* **]**

---

no

Indicates that internal logging is to be disabled for the options specified.

---

logging syslog *ip_address*

Specifies the IP address of a system log server on the network in IPv4 dotted-decimal or IPv6 colon-separated notation.

---

event-verbosity { min | concise | full }

Specifies the level of detail to use in logging of events. Detail level must be one of the following:

- **min**: Displays minimal detail.
- **concise**: Displays summary detail.
- **full**: Displays full detail.

---

facility *facilities*

Default: **local7**

Specifies the local facility for which the system logging server's logging options shall be applied. Local facility must be one of the following:

- **local0**
- **local1**
- **local2**
- **local3**
- **local4**
- **local5**
- **local6**
- **local7**

Multiple system log servers can share the logging options of a given local facility. This allows for the logical grouping of system log servers and the options which affect all of those associated with the same local facility.

pdu-data { none | hex | hex-ascii }

Specifies output format for packet data units when logged. Format must be one of the following:

- **none**: Displays data in raw format.
- **hex**: Displays data in hexadecimal format.
- **hex-ascii**: Displays data in hexadecimal and ASCII format (similar to a main-frame dump).

pdu-verbosity *pdu_level*

Specifies the level of verboseness to use in logging of packet data units as a value from 1 through 5, where 5 is the most detailed.

rate *value*

Specifies the rate at which log entries are allowed to be sent to the system log server. No more than the number specified by *value* will be sent to a system log server within any given one-second interval. *value* must be an integer from 0 through 100000. Default: 1000

Usage

Set the log servers to enable remote review of log data.

Example

The following sets the logging for events to the maximum for the local7 facility:

```
logging syslog 10.2.3.4 event-verbosity full
```

The following command sets the logging for packet data units to level 3 and sets the output format to the main-frame style hex-ascii for the local3 facility:

```
logging syslog 10.2.3.4 facility local3 pdu-data hex-ascii pdu-verbosity
3
```

The following sets the rate of information for the local1 facility:

```
logging syslog 10.2.3.4 facility local1 rate 100
```

The following disables internal logging to the system log server specified:

```
no logging syslog 10.2.3.4
```

mag-service

Creates a Mobile Access Gateway (MAG) service or specifies an existing MAG service and enters the MAG Service Configuration Mode for the current context.

Product

HSGW, S-GW

Privilege

Administrator

Syntax

mag-service *service_name* **[-noconfirm]**

no mag-service *service_name*

mag-service *service_name*

Specifies the name of the MAG service. If *service_name* does not refer to an existing service, the new service is created if resources allow.
service_name is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no mag-service *service_name*

Removes the specified MAG service from the context.

Usage

Enter the MAG Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your Cisco service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-mag-service)#
```

MAG Service Configuration Mode commands are defined in the *MAG Service Configuration Mode Commands* chapter.
Use this command when configuring the following eHRPD and PMIP SAE components: HSGW and S-GW.

Example

The following command enters the existing MAG Service Configuration Mode (or creates it if it does not already exist) for the service named *mag-service1*:

```
mag-service mag-service1
```

The following command will remove *mag-service1* from the system:

```
no mag-service mag-service1
```

map-service

Creates a Mobile Application Part (MAP) Service instance and enters the MAP Service Configuration mode to define or edit the MAP service parameters.

MAP is the SS7 protocol that provides the application layer required by some of the nodes in GPRS/UMTS networks to communicate with each other in order to provide services to mobile phone users. MAP is used by the serving GPRS support node (SGSN) to access SS7 network nodes such as a home location register (HLR) or a radio access network (RAN).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

map-service *srvc_name*

no map-service *srvc_name*

no

Remove the specified MAP service from the configuration for the current context.

map-service *srvc_name*

Specifies the name of the MAP service as a unique alphanumeric string of 1 through 63 characters.

Usage

Use this command to create, edit, or remove a MAP service configuration.

Important: For details about the commands and parameters, check the *MAP Service Configuration Mode Commands* chapter.

Example

The following command creates a MAP service named *map_1*:

```
map-service map_1
```

The following command removes the configuration for a MAP service named *map_1* from the configuration for the current context:

```
no map-service map_1
```

mme-service

Creates an Mobility Management Entity (MME) service or configures an existing MME service and enters the MME Service Configuration Mode for Evolved Packet Core (EPC) networks in the current context.

Product

MME

Privilege

Administrator

Syntax

mme-service *service_name* **[-noconfirm]**

no mme-service *service_name*

no

Removes the specified MME service from the context.

mme-service *service_name*

Specifies the name of the MME service. If *service_name* does not refer to an existing service, the new service is created if resources allow.
service_name is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Enter the MME Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 8 MME service can be configured on a system which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-mme-service)#
```

MME Service Configuration Mode commands are defined in the *MME Service Configuration Mode Commands* chapter.

Caution: This is a critical configuration. The MME service cannot be configured without this configuration. Any change to this configuration would lead to restarting the MME service and removing or disabling this configuration will stop the MME service.

Example

The following command enters the existing MME Service Configuration Mode (or creates it if it does not already exist) for the service named *mme-service1*:

```
mme-service mme-service1
```

The following command will remove *mme-service1* from the system:

```
no mme-service mme-service1
```

mobile-ip fa newcall

Configures settings that effect all FA services in the current context.

Product

FA

Privilege

Security Administrator, Administrator

Syntax

mobile-ip fa { multiple-dynamic-reg-per-nai | newcall duplicate-home-address { accept | reject } }

{ default | no } mobile-ip fa { multiple-dynamic-reg-per-nai | newcall duplicate-home-address }

---

default

Configures the default setting for the specified parameter.

- **multiple-dynamic-reg-per-nai**: All FA services in the current context can not simultaneously setup multiple dynamic home address registrations that have the same NAI.
- **newcall duplicate-home-address**: **reject**

---

no

- **multiple-dynamic-reg-per-nai**: Disables all FA services in the current context from simultaneously setting up multiple dynamic home address registrations that have the same NAI.
- **newcall duplicate-home-address**: Resets this option to its default of reject.

---

mobile-ip fa multiple-dynamic-reg-per-nai

This keyword allows all FA services in the current context to simultaneously setup multiple dynamic home address registrations that have the same NAI.

---

mobile-ip fa newcall duplicate-home-address { accept | reject }

- **accept**: The new call is accepted and the existing call is dropped.
- **reject**: The new call is rejected with an Admin Prohibited code.

Usage

Use this command to set the behavior of all FA services in the current context.

Example

To configure all FA services to accept new calls and drop the existing call when the new call requests an IP address that is already in use by an existing call, enter the following command:

```
mobile-ip fa newcall duplicate-home-address accept
```

To enable all FA services in the current context to allow all FA services in the current context to simultaneously setup multiple dynamic home address registrations that have the same NAI, enter the following command:

```
mobile-ip fa multiple-dynamic-reg-per-nai
```

mobile-ip ha assignment-table

Creates a Mobile IP HA assignment table and enters Mobile IP HA Assignment Table Configuration Mode.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

mobile-ip ha assignment-table *atable_name* **[-noconfirm]**

no mobile-ip ha assignment-table *atable_name*

no

This keyword deletes the specified assignment table

mobile-ip ha assignment-table *atable_name*

Specifies the name of the MIP HA assignment table to create or edit as an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to create a new MIP HA assignment table or edit an existing MIP HA assignment table.

Important: A maximum of eight MIP HA assignment tables can be configured per context with a maximum of 8 MIP HA assignment tables across all contexts.

Important: A maximum of 256 non-overlapping hoa-ranges can be configured per MIP HA Assignment table with a maximum of 256 non-overlapping hoa-ranges across all MIP HA Assignment tables.

Example

The following command creates a new MIP HA assignment table name *MIPHAtable1* and enters MIP HA Assignment Table Configuration Mode without asking for confirmation from the user:

```
mobile-ip ha assignment-table MIPHAtable1
```

mobile-ip ha newcall

Configures the behavior of all HA services when duplicate home addresses and duplicate IMSI sessions occur for new calls.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
mobile-ip ha newcall { duplicate-home-address { accept | reject } | duplicate-imsi-
session { allow | disallow | global-disallow } | wimax-session-overwrite {allow |
disallow }

{ default | no } mobile-ip ha newcall { duplicate-home-address | duplicate-imsi-session |
wimax-session-overwrite }
```

---

default

Configures the default setting for the specified parameter.

- **duplicate-home-address**: **reject**—sets HA services to reject a new call that requests an IP address that is already assigned.
- **duplicate-imsi-session**: **allow**—sets HA services to accept new calls that have the same IMSI as a call that is already active.
- **wimax-session-overwrite:disallow**—disable session overwrite feature for WiMax mobile-ip calls on the HA.

---

no

Configures the default setting for the specified parameter.

---

mobile-ip ha newcall duplicate-home-address { accept | reject }

Configures the HA to either accept or reject new calls if the new call requests a static IP home address that is already assigned to an existing call from an IP address pool in the same destination context.

- **accept**: The new call is accepted and the existing call is dropped.
- **reject**: The new call is rejected with an Admin Prohibited code.

---

mobile-ip ha newcall duplicate-imsi-session { allow | disallow | global-disallow }

Configures the HA to either permit or not permit multiple sessions for the same IMSI.

- **allow**: Allows multiple sessions for the same IMSI.
- **disallow**: If a mobile node already has an active session and a new sessions is requested using the same IMSI, the currently active session is dropped and the new session is accepted.
- **global-disallow**: Enables HA services in this context to accept a new session and disconnect any other session(s) having the same IMSI being processed in this context. In addition, a request is sent to all other contexts containing HA services to do the same.

Important: In order to ensure a single session per IMSI across all contexts containing HA services, the global-disallow option must be configured in every context.

mobile-ip ha newcall wimax-session-overwrite { allow | disallow }

Use this command to enable or disable the overwrite feature for WiMAX mobile ip (MIPv4) calls on the HA.

Usage

Use this command to set the behavior of all HA services for new calls.

Example

To configure all HA services to accept new calls when the new call requests a static IP that is already assigned from an IP pool in the same destination context, enter the following command:

```
mobile-ip ha newcall duplicate-home-address accept
```

To configure all HA services to drop an active call and accept a new one that uses the same IMSI, enter the following command:

```
mobile-ip ha newcall duplicate-imsi-session disallow
```

mobile-ip ha reconnect

Sets the behavior of all HA services to reconnect dropped calls.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] mobile-ip ha reconnect [ static-homeaddr [ dynamic-pool-allocation ] ] }
```

mobile-ip ha reconnect

Reconnects dropped HA calls.

static-homeaddr

Specifies that the home address as a static IP address.

dynamic-pool-allocation

Allows a dynamic pool to accept a static address allocation.

Usage

Use this command to reset the HA behavior for new calls.

Example

```
mobile-ip ha reconnect

mobile-ip ha reconnect static-homeaddr

mobile-ip ha reconnect static-homeaddr dynamic-pool-allocation

no mobile-ip ha reconnect

no mobile-ip ha reconnect static-homeaddr
```

mpls bgp forwarding

Globally enables Multiprotocol Label Switching (MPLS) Border Gateway Protocol (BGP) forwarding.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] mpls bgp forwarding
```

no

Disables MPLS BGP forwarding.

mpls bgp

Enables MPLS BGP forwarding.

Usage

Use this command to globally enable the MPLS BGP forwarding. By enabling this command, the BGP VPNv4 routes need not have an underlying LSP to forward the IP packets. If this command is not enabled, then the nexthop for the BGP routes must be reachable via LDP.

Caution: This command should be enabled ONLY when all the BGP peering where VPNv4 routes are exchanged are one hop away.

Example

The following command enables the MPLS BGP forwarding on the system:

```
mpls bgp forwarding
```

mpls ip

Globally enables the Multiprotocol Label Switching (MPLS) forwarding of IPv4 packets along normally routed paths.

Product

GGSN, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] mpls ip
```

no

Disables MPLS forwarding of IPv4 packets configured on the system. **no mpls ip** stops dynamic label distribution on all the interfaces irrespective of interface configuration.

mpls ip

Enables MPLS forwarding of IPv4 packets configured on the system. It starts dynamic label distribution on all the interfaces irrespective of interface configuration.

Usage

Use this command to globally enable the MPLS forwarding of IPv4 packets along normally routed paths for the whole context. It still does not start label distribution over an interface until MPLS has been enabled for the interface as well. This command changes the context to MPLS IP configuration mode for MPLS protocols specific configuration.

Caution: This feature is not enabled by default.

Example

Following command enables MPLS forwarding of IPv4 packets along normally routed paths:

```
mpls ip
```

mseg-service

This command allows you to create/configure/delete a Mobile Services Edge Gateway (MSEG) service.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

mseg-service *mseg_service_name* **[-noconfirm]**

no mseg-service *mseg_service_name*

no

If previously configured, deletes the specified MSEG service from the current context.

mseg_service_name

Specifies the MSEG service to add/configure/delete.
mseg_service_name must be the name of an MSEG service, and must be an alphanumeric string of 1 through 63 characters.
If the named MSEG service does not exist, it is created and the CLI mode changes to the MSEG Service Configuration Mode wherein the MSEG service can be configured.
If the named MSEG service already exists, the CLI mode changes to the MSEG Service Configuration Mode for that MSEG service.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to create/configure/delete an MSEG service.
Entering this command results in the following prompt:
`[context_name]hostname(config-mseg-service)#`
MSEG service configuration commands are described in the *MSEG Service Configuration Mode Commands* chapter.

Example

The following command creates an MSEG service named *test*, and enters the MSEG Service Configuration Mode:

```
mseg-service test
```

nw-reachability server

Adds or deletes a reachability-detect server and configures parameters for retrying the failure-detection process. When network reachability is enabled, an ICMP ping request is sent to this device. If there is no response after a specified number of retries, the network is deemed failed. Execute this command multiple times to configure multiple network reachability servers.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

nw-reachability server *server_name* **[interval** *seconds* **] [local-addr** *ip_addr* **] [num-retry** *num* **] [remote-addr** *ip_addr* **] [timeout** *seconds***]**

no nw-reachability server *server_name*

no

Delete the reference to the specified network reachability server.

nw-reachability server *server_name*

Specifies the name for the network device that is sent ping packets to test for network reachability.

interval *seconds*

Specifies the frequency in seconds for sending ping requests. as an integer from 1 through 3600. Default: 60

local-addr *ip_addr*

Specifies the IP address to be used as the source address of the ping packets; If this is unspecified, an arbitrary IP address that is configured in the context is used. *ip_addr* must be entered using IPv4 dotted-decimal notation.

num-retry *num*

Specifies the number of retries before deciding that there is a network-failure. as an integer from 0 through 100. Default: 5

remote-addr *ip_addr*

Specifies the IP address of a network element to use as the destination to send the ping packets for detecting network failure or reachability. *ip_addr* must be entered using IPv4 dotted-decimal notation.

timeout *seconds*

Specifies how long to wait (in seconds) before retransmitting a ping request to the remote address as an integer from 1 through 1. Default: 3

Usage

Use this command to set up a network device on a destination network that is used ensure that Mobile IP sessions can reach the required network from the HA.

Important: Refer to the HA Configuration Mode command **`policy nw-reachability-fail`** to configure the action that should be taken when network reachability fails.

Important: Refer to the Subscriber Config Mode command **`nw-reachability-server`** to bind the network reachability to a specific subscriber.

Important: Refer to the **`nw-reachability server server_name`** keyword of the **`ip pool`** command in this chapter to bind the network reachability server to an IP pool.

Example

To set a network device called InternetDevice with the IP address of *`192.168.100.10`* as the remote address that is pinged to determine network reachability and use the address *`192.168.200.10`* as the origination address of the ping packets sent, enter the following command:

```
nw-reachability server InternetDevice local-addr 192.168.200.10 remote-
addr 192.168.100.10
```

network-requested-pdp-context activate

Configures the mobile station(s) (MSs) for which network initiated PDP contexts are supported.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

network-requested-pdp-context activate address *ip_address* **dst-context** *context_name* **imsi** *imsi* **apn** *apn_name*

no network-requested-pdp-context activate address *ip_address* **dst-context** *context_name*

no

Disables the system's ability to accept network-requested PDP contexts on the specified interface.

network-requested-pdp-context activate address *ip_address*

Specifies the static IP address of the MS n IPv4 dotted-decimal notation.

dst-context *context_name*

Specifies the name of the destination context configured on the system containing the static IP address pool in which the MS's IP address is configured. *context_name* is an alphanumeric string of 1 through 79 characters that is case sensitive.

imsi *imsi*

Specifies the International Mobile Subscriber Identity (IMSI) of the MS as a string of 1 through 15 numeric characters

apn *apn_name*

Specifies the Access Point Name (APN) that is passed to the SGSN by the system. *apn_name* is an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage

Use this command to specify the MS(s) for which network initiated PDP contexts are supported.
When a packet is received for an MS that does not currently have a PDP context established, the system checks the configuration of this parameter to determine if the destination IP address specified in the packet is specified by this parameter. If the address is not specified, then the system discards the packet. If the address is specified, the system uses the configured IMSI and APN to determine the appropriate SGSN from the Home Location Register (HLR). The system communicates with the HLR through the interworking node configured using the network-requested-pdp-context gsn-map command.
Once the session is established, the destination context specified by this command is used in place of the one either configured within the specified APN template or returned by a RADIUS server during authentication.
This command can be issued multiple times supporting network initiated PDP contexts for up to 1,000 configured addresses per system context.

Example

The following command enables support for network initiated PDP contexts for an MS with a static IP address of *20.13.5.40* from a pool configured in the destination context pdn1 with an IMSI of *3319784450* that uses an APN template called *isp1*:

```
network-requested-pdp-context activate address 20.13.5.40 dst-context
pdn1 imsi 3319784450 apn isp1
```

network-requested-pdp-context gsn-map

Configures the IP address of the interworking node that is used by the system to communicate with the Home Location Register (HLR), and optionally sets the GTP version to use.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

network-requested-pdp-context gsn-map *ip_address* **[gtp-version { 0 | 1 }]**

no network-requested-pdp-context gsn-map

no

Deletes a previously configured gsn-map node.

network-requested-pdp-context gsn-map *ip_address*

Specifies the IP address of the gsn-map node in Pv4 dotted-decimal or IPv6 colon-separated notation.

gtp-version { 0 | 1 }

Specifies the gtp version used. Default: 1

Usage

Communications from the system to the HLR must go through a GSN-map interworking node that performs the protocol conversion from GTPC to SS7.
The UDP port for this communication is 2123.
Support for network requested PDP contexts must be configured within source contexts on the system. Only one gsn-map node can be configured per source context.
The source context also contains the GGSN service configuration that specifies the IP address of the Gn interface. If multiple GGSN services are configured in the source context, one is selected at random for initiating the Network Requested PDP Context Activation procedure.
Communication with the gsn-map node is done over the Gn interface configured for the GGSN service. The IP address of that interface is used as the system's source address.

Example

The following command configures the system to communicate with a gsn-map node having an IP address of *192.168.2.5*:

```
network-requested-pdp-context gsn-map 192.168.2.5
```

network-requested-pdp-context hold-down-time

Configures the time duration to that the system will wait after the SGSN rejects an attempt for a network-requested PDP context creation for the subscriber.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

network-requested-pdp-context hold-down-time *time*

default network-requested-pdp-context hold-down-time

default

Configures the default setting.
Default: 60 seconds

network-requested-pdp-context hold-down-time *time*

Specifies the time interval (in seconds) as an integer from 0 through 86400.

Usage

Packets received during this time period would be discarded, rather than being used to cause another network-requested PDP context creation attempt for the same subscriber. After the time period has expired, any subsequent packets received would cause another network-requested PDP context creation procedure to begin.

Example

The following command configures a hold-down-time of *120* seconds:

```
network-requested-pdp-context hold-down-time 120
```

network-requested-pdp-context interval

Configures the minimum amount of time that must elapse between the deletion of a network initiated PDP context and the creation of a new one for the same MS.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

network-requested-pdp-context interval *time*

default network-requested-pdp-context interval

default

Returns the command to its default setting of 60.

network-requested-pdp-context interval *time*

Specifies the minimum amount of time (in seconds) that must pass before the system allows another network-requested PDP context for a specific MS after the previous context was deleted. *time* is an integer from 0 through 86400. Default: 60

Usage

Once an MS deletes a PDP context that initiated from the network, the system automatically waits the amount of time configured by this parameter before allowing another network initiated PDP context for the same MS.

Example

The following command specifies that the system waits *120* seconds before allowing another network requested PDP context for an MS:

```
network-requested-pdp-context interval 120
```

network-requested-pdp-context sgsn-cache-time

Configures the time duration that the GGSN keeps the SGSN/subscriber pair cached in its local memory.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

network-requested-pdp-context sgsn-cache-time *time*

default network-requested-pdp-context sgsn-cache-time

default

Configures the default setting.
Default: 300 seconds

network-requested-pdp-context sgsn-cache-time *time*

Specifies the time interval (in seconds) as an integer from 0 through 86400.

Usage

For an initial network-requested PDP context creation, the system contacts the HLR (via the GSN-MAP interworking node) to learn which SGSN is currently servicing the subscriber. The system keeps that information in cache memory for the configured time, so that future network-requested PDP context creations for that subscriber can be initiated without having to contact the HLR again.

Example

The following command configures an sgsn-cache-time of *500* seconds:

```
network-requested-pdp-context sgsn-cache-time 500
```

operator

Configures a context-level operator account within the current context.

Product

All

Privilege

Security Administrator

Syntax

operator *user_name* **[encrypted] password** *password* **[ecs] [expiry-date** *date_time* **] [li-administration**] **[noecs] [timeout-absolute** *abs_seconds* **] [timeout-min-absolute** *abs_minutes* **] [timeout-idle** *timeout_duration* **] [timeout-min-idle** *idle_minutes* **]**

no operator *user_name*

no

Removes a previously configured context-level operator account.

operator *user_name*

Specifies a name for the account as an alphanumeric string of 1 through 32 characters.

[encrypted] password *password*

Specifies the password to use for the user which is being given context-level operator privileges within the current context. The **encrypted** keyword indicates the password specified uses encryption.
password is an alphanumeric string of 1 through 63 characters without encryption, or 1 through 127 with encryption.
The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

ecs

Permits the specific user to access ACS-specific configuration commands from Exec Mode only. Default: ACS-specific configuration commands are not allowed.

expiry-date *date_time*

Specifies the date and time that this account expires. Enter the date and time in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.
Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

li-administration

Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

noecs

Prevents the user from accessing ACS-specific configuration commands. Default: Enabled

timeout-absolute *abs_seconds*

This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.
Specifies the maximum amount of time (in seconds) the context-level operator may have a session active before the session is forcibly terminated. *abs_seconds* must be a value in the range from 0 through 300000000. The value 0 disables the absolute timeout. Default: 0

timeout-min-absolute *abs_minutes*

Specifies the maximum amount of time (in minutes) the context-level operator may have a session active before the session is forcibly terminated. *abs_minutes* must be an integer from 0 through 300000000. The value 0 disables the absolute timeout. Default: 0

timeout-idle *timeout_duration*

This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.
Specifies the maximum amount of idle time (in seconds) the context-level operator may have a session active before the session is terminated. *timeout_duration* must be an integer from 0 through 300000000. The value 0 disables the idle timeout. Default: 0

timeout-min-idle *idle_minutes*

Specifies the maximum amount of idle time (in minutes) the context-level operator may have a session active before the session is terminated. *idle_minutes* must be an integer from 0 through 300000000. The value 0 disables the idle timeout. Default: 0

Usage

Use this command to create new context-level operator or modify existing operator's options, in particular, the timeout values.
Operators have read-only privileges. They can maneuver across multiple contexts, but cannot perform configuration operations. Refer to the *Command Line Interface Overview* chapter for more information.

Important: A maximum of 128 administrative users and/or subscribers may be locally configured per context.

Example

The following command creates a context-level operator account named *user1* with ACS control:

```
operator user1 password secretPassword ecs
```

The following command removes a previously configured context-level operator account named *user1*:

```
no operator user1
```

optimize pdsn inter-service-handoff

Controls the optimization of the system's handling of inter-PDSN handoffs.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] optimize pdsn inter-service-handoff
```

default

Resets the command to its default setting of enabled.

no

Disables the feature.

optimize pdsn inter-service-handoff

Enables system optimization of the handling of inter-PDSN handoffs.

Usage

When more than one PDSN service is defined in a context, each PDSN-Service acts as an independent PDSN. When a Mobile Node (MN) moves from one PDSN service to another PDSN service, by rule, it is an inter-PDSN handoff. This command optimizes PDSN handoffs between PDSN Services that are defined in the same context in the system.

The default for this parameter is enabled. The no keyword disables this functionality.

When enabled, the system treats handoffs happening between two PDSN services in the same context as an inter-PDSN handoff. Existing PPP session states and connection information is reused. If the inter-PDSN handoff requires a PPP restart, then PPP is restarted. The optimized inter-service-handoff may not restart the PPP during handoffs allowing the MN to keep the same IP address for the Simple IP session.

Example

```
optimize pdsn inter-service-handoff
```

pcc-af-service

Creates or removes an IPCF Policy and Charging Control (PCC) Application Function (AF) service or configures an existing PCC-AF service. It enters the PCC-AF Service Configuration Mode to link, configure, and manage the Application Function endpoints and associated PCC services over the Rx interface for the IPCF services.

Product

IPCF

Privilege

Administrator

Syntax

pcc-af-service *service_name* [**-noconfirm**]

no pcc-af-service *service_name*

no

Removes the specified PCC-AF service from the context.

pcc-af-service *service_name*

Specifies the name of the PCC-AF service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to enter the PCC-AF Service Configuration Mode for an existing service or for a newly defined PCC-AF service. This command is also used to remove an existing service.
The PCC-AF-Service consolidates the provisioning and management required for the PCC-AF services being supported by the network that fall under the PCC regime. The application service handles the **Rx** interface over which the IPCF may receive media information for the application usage from AF.

Important: In the absence of an Rx interface, the media information is available in the PCC-AF Service statically.

A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-imsapp-service)#
```

The commands available in this mode are defined in the *PCC -AF Service Configuration Mode Commands* chapter.

Caution: This is a critical configuration. The PCC-AF service cannot be configured without this configuration. Any change to this configuration would lead to restarting the PCC-AF service and removing or disabling this configuration will stop the PCC-AF service.

Example

The following command enters the existing PCC-AF Service Configuration Mode (or creates it if it does not already exist) for the service named *af-service1*:

```
pcc-af-service af-service1
```

The following command will remove *af-service1* from the system:

```
no pcc-af-service af-service1
```

pcc-policy-service

Creates or removes an IPCF PCC-Policy service or configures an existing PCC-Policy service. It enters the PCC-Policy Service Configuration Mode to link, configure, and manage the Gx interface endpoints for policy authorization where IPCF acts as a policy server.

Product

IPCF

Privilege

Administrator

Syntax

pcc-policy-service *service_name* [**-noconfirm**]

no pcc-policy-service *service_name*

no

Removes the specified PCC-Policy service from the context.

pcc-policy-service *service_name*

Specifies the name of the PCC-Policy service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to enter the PCC-Policy Service Configuration Mode for an existing service or for a newly defined PCC-Policy service. This command is also used to remove an existing service.
The PCC-Policy-Service is mainly used to provide a mechanism to manage the external Gx or similar interfaces required for policy authorization purpose. It manages Gx and Gx-like interfaces such as Gxc/Gxa between IPCF/PCRF and PCEF or BBERF, which is based on the dictionary used for PCC.
Multiple instances of PCC-Policy-Service may exist in a system which could link with the same PCC-Service that controls the business logic. This service allows for management of configuration for peers as well self related to Gx like functions.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-pccpolicy-service)#
```

The commands available in this mode are defined in the *PCC-Policy Service Configuration Mode Commands* chapter.

Caution: This is a critical configuration. The PCC-Policy service cannot be configured without this configuration. Any change to this configuration would lead to restarting the PCC-Policy service and removing or disabling this configuration will stop the PCC-Policy service.

Example

The following command enters the existing PCC-Policy Service Configuration Mode (or creates it if it does not already exist) for the service named *gx-service1*:

```
pcc-policy-service gx-service1
```

The following command will remove *gx-service1* from the system:

```
no pcc-policy-service gx-service1
```

pcc-service

Creates or removes an IPCF Policy and Charging Control (PCC) service or configures an existing PCC service. It enters the PCC Service Configuration Mode for IPCF related configurations in the current context.

Product

IPCF

Privilege

Administrator

Syntax

pcc-service *service_name* [**-noconfirm**]

no pcc-service *service_name*

no

Removes the specified PCC service from the context.

pcc-service *service_name*

Specifies the name of the PCC service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to enter the PCC Service Configuration Mode for an existing service or for a newly defined PCC service. This command is also used to remove an existing service.
The IPCF PCC Service Configuration Mode is used to link, consolidate and manage the policy logic for the networks. The authorization of resources for a subscriber's data usage under various conditions and policies are defined in the IPCF PCC service.
Only one PCC service can be configured on a system which is further limited to a maximum of 256 services (regardless of type) configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-service)#
```

The commands available in this mode are defined in the *PCC Service Configuration Mode Commands* chapter.

Caution: This is a critical configuration. The PCC service cannot be configured without this configuration. Any change to this configuration would lead to restarting the Policy and Charging Control service and removing or disabling this configuration will stop the PCC service.

Example

The following command enters the existing PCC Service Configuration Mode (or creates it if it does not already exist) for the service named *ipcf-service1*:

```
pcc-service ipcf-service1
```

The following command will remove *ipcf-service1* from the system:

```
no pcc-service ipcf-service1
```

pcc-sp-endpoint

Creates or removes an IPCF PCC Sp interface endpoint or configures an existing PCC Sp interface client endpoint. It enters the PCC Sp Endpoint Configuration Mode to link, configure, and manage the operational parameters related to its peer.

Product

IPCF

Privilege

Administrator

Syntax

pcc-sp-endpoint *sp_intfc1* **[-noconfirm]**

no pcc-sp-endpoint *sp_intfc1*

no

Removes the specified PCC Sp interface endpoint from the context.

pcc-sp-endpoint *sp_intfc1*

Specifies the name of the PCC Sp interface endpoint. If *sp_intfc_endpoint* does not refer to an existing endpoint, the new endpoint is created if resources allow. *sp_intfc_endpoint* is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to enter the PCC-Sp-Endpoint Configuration Mode for an existing interface or for a newly defined PCC **Sp** interface endpoint. This command is also used to remove an existing endpoints.
An instance of PCC Sp endpoint represent a client end for SSC/SPR interactions. It is possible to support multiple Sp endpoints each supporting the same or different protocol. The PCC Sp endpoint facilitates the configuration of the treatment required of the Sp interface as well as manage the connection and operational parameters related to its peer.
Only one PCC Sp endpoint across a chassis can be configured on a system.
Entering this command results in the following prompt:

```
[context_name]hostname(config-spendpoint)#
```

The commands available in this mode are defined in the *PCC-Sp-Endpoint Configuration Mode Commands* chapter.

Caution: This is a critical configuration. The PCC Sp endpoint cannot be configured without this configuration. Any change to this configuration would lead to reset the PCC Sp interface and removing or disabling this configuration also disables the PCC Sp interface.

Example

The following command enters the existing PCC Sp Endpoint Configuration Mode (or creates it if it does not already exist) for the endpoint named *sp_intfc1*:

```
pcc-sp-endpoint sp_intfc1
```

The following command will remove *sp_intfc1* from the system:

```
pcc-sp-endpoint sp_intfc1
```

pdg-service

Creates a new PDG service or specifies an existing PDG service and enters the PDG Service Configuration Mode. A maximum of 16 PDG services can be created. This limit applies per ASR 5000 chassis and per context.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

no pdg-service *name*

pdg-service *name*

Specifies the name of a new or existing PDG service as an alphanumeric string 1 through 63 characters that must be unique across all FNG services within the same context and across all contexts.

no pdg-service *name*

Deletes the specified PDG service.

Usage

Use this command in Context Configuration Mode to create a new PDG service or modify an existing one. Executing this command enters the PDG Service Configuration Mode.

Example

The following command configures an PDG service named *pdg_service_1* and enters the PDG Service Configuration Mode:

```
pdg-service pdg_service_1
```

pdif-service

Creates a new, or specifies an existing, Packet Data Interworking Function (PDIF) service and enters the PDIF Service Configuration Mode.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

`[ no ] pdif-service` *`name`* **`[ -noconfirm ]`**

`pdif-service` *`name`*

Specifies the name of a new or existing PDIF service as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to create a new or enter an existing PDIF service.
Entering this command results in the following prompt:
[*`context_name`*]*`hostname`*(config-pdif-service)#
PDIF Service Configuration Mode commands are defined in the *PDIF Service Configuration Mode Commands* chapter.

Example

The following command configures a PDIF service called *`pdif2`* and enters the PDIF Service Configuration Mode:

```
pdif-service pdif2
```

pdsn-service

Creates or deletes a packet data service or specifies an existing PDSN service for which to enter the Packet Data Service Configuration Mode for the current context.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] pdsn-service name
```

no

Indicates the packet data service specified is to be removed.

pdsn-service *name*

Specifies the name of the PDSN service to configure. If *name* does not refer to an existing service, the new service is created if resources allow. *name* is an alphanumeric string of 1 through 63 characters.

Usage

Enter the PDSN Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your Cisco service representative for more information.

Example

The following command will enter the PDSN Service Configuration Mode creating the service *sampleService*, if necessary.

```
pdsn-service sampleService
```

The following command will remove *sampleService* as being a defined PDSN service.

```
no pdsn-service sampleService
```

pgw-service

Creates an PDN-Gateway (P-GW) service or specifies an existing P-GW service and enters the P-GW Service Configuration Mode for the current context.

Product

P-GW

Privilege

Administrator

Syntax

pgw-service *service_name* **[-noconfirm]**

no pgw-service *service_name*

pgw-service *service_name*

Specifies the name of the P-GW service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no pgw-service *service_name*

Removes the specified P-GW service from the context.

Usage

Enter the P-GW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-pgw-service)#
```

P-GW Service Configuration Mode commands are defined in the *P-GW Service Configuration Mode Commands* chapter.
Use this command when configuring the following eHRPD and SAE components: P-GW.

Example

The following command enters the existing P-GW Service Configuration Mode (or creates it if it does not already exist) for the service named *pgw-service1*:

```
pgw-service pgw-service1
```

The following command will remove *pgw-service1* from the system:

```
no pgw-service pgw-service1
```

pilot-packet

Configures pilot packets containing key pieces of information about a subscriber session to third party network elements.

Product

PDSN, HA

Privilege

Administrator

Syntax

```
pilot-packet source-ip-address source_ip_address destination-ip-address
destination_ip_address destination-udp-port udp_port_valueno pilot-packet
```

no

Disables Pilot packet option.

pilot-packet source-ip-address *source_ip_address*

Specifies the IP addresses for the sourcing and terminating Pilot Packets. The IP address must entered using IPv4 dotted-decimal or IPv6 colon-separated notation.

- *source_ip_address*: Specifies the IP address of the source for sending Pilot Packets.
- *destination_ip_address*: Specifies the IP address of the destination for the Pilot Packets.

destination-udp-port *udp_port_value*

Specifies the UDP port value as an integer from 1 through 65535.

Usage

Use this command to configure Pilot-Packet parameters.

Example

The following command configures pilot packets with source and destination IPv4/IPv6 addresses along with the destination port:

```
pilot-packet source-ip-address 10.2.3.4 destination-ip-address 10.3.4.5
destination-udp-port 221
```

policy

Enters an existing accounting policy or creates a new one where accounting parameters are configured.

Product

HSGW, P-GW, S-GW

Privilege

Administrator

Syntax

[no] policy accounting *name*

no

Removes the specified accounting policy from the context.

policy accounting *name*

Specifies the name of the existing or new accounting policy as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to enter the Accounting Policy Configuration mode to edit an existing accounting policy or configure an new policy.
Entering this command results in the following prompt:

```
[context_name]hostname(config-accounting-policy)#
```

Accounting Policy Configuration Mode commands are defined in the *Accounting Policy Configuration Mode Commands* chapter.

Example

The following command enters the Accounting Policy Configuration Mode for a policy named *acct5*:

```
policy accounting acct5
```

policy-group

Creates or deletes a policy group. It enters the Policy-Group Configuration Mode within the current destination context for flow-based traffic policing to a subscriber session flow.

Product

PDSN, HA, ASN-GW, HSGW

Privilege

Security Administrator, Administrator

Syntax

[no] policy-group name *policy_group*

no

Deletes configured policy group within the context.

policy-group name *policy_group*

Specifies the name of Policy-Group as an alphanumeric string of 1 through 15 characters that is case sensitive.

Usage

Use this command to form a policy group from a set of configured Policy-Maps. A policy group supports up to 16 policies for a subscriber session flow.

Example

The following command configures a policy group *policy_group1* for a subscriber session flow:

```
policy-group name policy_group1
```

policy-map

Creates or deletes a policy map. It enters the Traffic Policy-Map Configuration Mode within the current destination context to configure the flow-based traffic policing for a subscriber session flow.

Product

PDSN, HA, ASN-GW, HSGW

Privilege

Security Administrator, Administrator

Syntax

[no] policy-map name *policy_name*

no

Deletes configured Policy-Map within the context.

policy-map name *policy_name*

Specifies the name of Policy-Map as an alphanumeric string of 1 through 15 characters that is case sensitive.

Usage

Use this command to enter Traffic Policy-Map Configuration Mode and to set the Class-Map and corresponding traffic flow treatment to traffic policy for a subscriber session flow.

Example

Following command configures a policy map *policy1* where other flow treatments is configured.

```
policy-map name policy1
```

ppp

Configures point-to-point protocol parameters for the current context.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

ppp { acfc { receive { allow | deny } | transmit { apply | ignore | reject} } | auth-retry suppress-aaa-auth | chap fixed-challenge-length *length* **| dormant send-lcp-terminate | echo-max-retransmissions** *num_retries* **| echo-retransmit-timeout** *msec* **| first-lcp-retransmit-timeout** *milliseconds* **| lcp-authentication-discard retry-alternate** *num_discard* **| lcp-authentication-reject retry-alternate | lcp-start-delay** *delay* **| lcp-terminate connect-state | lcp-terminate mip-lifetime-expiry | lcp-terminate mip-revocation | max-authentication-attempts** *num* **| max-configuration-nak** *num* **| max-retransmissions** *number* **| max-terminate** *number* **| mru** *packet_size* **| negotiate default-value-options | peer-authentication** *user_name* **[encrypted] password** *password* **] | pfc { receive { allow | deny } | transmit { apply | ignore | reject} } | reject-peer-authentication | renegotiation retain-ip-address | retransmit-timeout** *milliseconds* **}**

no ppp { auth-retry suppress-aaa-auth | chap fixed-challenge-length | dormant send-lcp-terminate | lcp-authentication-descard retry-alternate *num_discard* **| lcp-authentication-reject retry-alternate | lcp-start-delay | lcp-terminate connect-state | reject-peer-authentication | renegotiation retain-ip-address }**

default lcp-authentication-descard retry-alternate *num_discard*

---

default

Restores the system defaults for the specific command/keyword.

---

no ppp { auth-retry suppress-aaa-auth | chap fixed-challenge-length | dormant send-lcp-terminate | lcp-authentication-discard retry-alternate *num_discard* **| lcp-authentication-reject retry-alternate | lcp-start-delay | lcp-terminate connect-state | lcp-terminate mip-lifetime-expiry | lcp-terminate mip-revocation | negotiate default-value-options | reject-peer-authentication | renegotiation retain-ip-address }**

Disables, deletes, or resets the specified option.
For **no ppp renegotiation retain-ip-address** the initially allocated IP address will be released and a new IP address will be allocated during PPP renegotiation.

---

ppp acfc { receive { allow | deny } | transmit { apply | ignore | reject} }

Configures PPP Address and Control Field Compression (ACFC) parameters.
receive { allow | deny }
This keyword specifies whether to allow Address and Control Field Compressed PPP packets received from the Peer. During LCP negotiation, the local PPP side indicates whether it can handle ACFC compressed PPP packets. Default: **allow**

When allow is specified, the local PPP side indicates that it can process ACFC compressed PPP packets and compressed packets are allowed. When deny is specified, the local PPP side indicates that it cannot handle ACFC compressed packets and compressed packets are not allowed.

transmit { apply | ignore | reject }

Specifies how Address and Control Field Compression should be applied for PPP packets transmitted to the Peer. During LCP negotiation, the Peer indicates whether it can handle ACFC compressed PPP packets.

Default: **ignore**

When apply is specified, if the peer requests ACFC, the request is accepted and ACFC is applied for transmitted PPP packets. When ignore is specified, if the peer requests ACFC, the request is accepted, but ACFC is not applied for transmitted PPP packets. When reject is specified, if the peer requests ACFC, the request is rejected and ACFC is not applied to transmitted packets.

---

auth-retry suppress-aaa-auth

This option does not allow PPP authentication retries to the AAA server after the AAA server has already authenticated a session. PPP locally stores the username and password, or challenge response, after a successful PPP authentication. If the Mobile Node retries the PAP request or CHAP-Response packet to the PDSN, PPP locally compares the incoming username, password or Challenge Response with the information stored from the previous successful authentication. If it matches, PAP ACK or CHAP Success is sent back to the Mobile Node, without performing AAA authentication. If the incoming information does not match with what is stored locally, then AAA authentication is attempted. The locally stored PPP authentication information is cleared once the session reaches a connected state.

Default: **no auth-retry suppress-aaa-auth**

Important: This option is not supported in conjunction with the GGSN product.

---

chap fixed-challenge-length *length*

Normally PPP CHAP uses a random challenge length from 17 to 32 bytes. This command allows you to configure a specific fixed challenge length of from 4 through 32 bytes. *length* must be an integer from 4 through 32.

Default: Disabled. PAP CHAP uses a random challenge length.

---

dormant send-lcp-terminate

Indicates a link control protocol (LCP) terminate message is enabled for dormant sessions.

Important: This option is not supported in conjunction with the GGSN product.

---

echo-max-retransmissions *num_retries*

Configures the maximum number of retransmissions of LCP ECHO_REQ before a session is terminated in an always-on session. *num_retries* must be an integer from 1 through 16. Default: 3

---

echo-retransmit-timeout *msec*

Configures the timeout (in milliseconds) before trying LCP ECHO_REQ for an always-on session. *msec* must be an integer from 100 through 5000. Default: 3000

first-lcp-retransmit-timeout *milliseconds*

Specifies the number of milliseconds to wait before attempting to retransmit control packets. This value configures the first retry. All subsequent retries are controlled by the value configured for the ppp **retransmit-timeout** keyword.
milliseconds must be an integer from 100 through 5000. Default: 3000

lcp-authentication-discard retry-alternate *num_discard*

Sets the number of discards up to which authentication option is discarded during LCP negotiation and retries starts to allow alternate authentication option. *num_discard* must be an integer from 0 through 5. Recommended value is 2. Default: Disabled.

lcp-authentication-reject retry-alternate

Specifies the action to be taken if the authentication option is rejected during LCP negotiation and retries the allowed alternate authentication option.
Default: Disabled. No alternate authentication option will be retried.

lcp-start-delay *delay*

Specifies the delay (in milliseconds) before link control protocol (LCP) is started. *delay* must be an integer from 0 through 5000. Default: 0

lcp-terminate connect-state

Enables sending an LCP terminate message to the Mobile Node when a PPP session is disconnected if the PPP session was already in a connected state.
Note that if the no keyword is used with this option, the PDSN must still send LCP Terminate in the event of an LCP/PCP negotiation failure or PPP authentication failure, which happens during connecting state.

Important: This option is not supported in conjunction with the GGSN product.

lcp-terminate mip-lifetime-expiry

Configures the PDSN to send an LCP Terminate Request when a MIP Session is terminated due to MIP Lifetime expiry (default).
Note that if the no keyword is used with this option, the PDSN does not send a LCP Terminate Request when a MIP session is terminated due to MIP Lifetime expiry.

lcp-terminate mip-revocation

Configures the PDSN to send a LCP Terminate Request when a MIP Session is terminated due to a Revocation being received from the HA (default).
Note that if the no keyword is used with this option, the PDSN does not send a LCP Terminate Request when a MIP session is terminated due to a Revocation being received from the HA.

max-authentication-attempts *num*

Configures the maximum number of time the PPP authentication attempt is allowed. *num* must be an integer from 1 through 10. Default: 1

max-configuration-nak *num*

This command configures the maximum number of consecutive configuration REJ/NAKs that can be sent during CP negotiations, before the CP is terminated. *num* must be an integer from 1 through 20. Default: 10

max-retransmission *number*

Specifies the maximum number of times control packets will be retransmitted. *number* must be an integer from 1 through 16. Default: 5

max-terminate *number*

Sets the maximum number of PPP LCP Terminate Requests transmitted to the Mobile Node. *number* must be an integer from 0 through 16. Default: 2

Important: This option is not supported in conjunction with the GGSN product.

mru *packet_size*

Specifies the maximum packet size that can be received in bytes. *packet_size* must be an integer from 128 through 1500. Default: 1500

negotiate default-value-options

Enables the inclusion of configuration options with default values in PPP configuration requests. Default: Disabled
The PPP standard states that configuration options with default values should not be included in Configuration Request (LCP, IPCP, etc.) packets. If the option is missing in the Configuration Request, the peer PPP assumes the default value for that configuration option.
When **negotiate default-value-options** is enabled, configuration options with default values are included in the PPP configuration Requests.

peer-authenticate *user_name* **[[encrypted] password** *password* **]**

Specifies the user name and an optional password required for point-to-point protocol peer connection authentications. *user_name* is an alphanumeric string of 1 through 63 characters. The keyword **password** is optional and if specified *password* is an alphanumeric string of 1 through 63 characters. The password specified must be in an encrypted format if the optional keyword **encrypted** was specified.
The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

pfc { receive { allow | deny } | transmit { apply | ignore | reject} }

Configures Protocol Field Compression (PFC) parameters.
receive { allow | deny } Default: **allow**
This keyword specifies whether to allow Protocol Field Compression (PFC) for PPP packets received from the peer. During LCP negotiation, the local PPP side indicates whether it can handle Protocol Field Compressed PPP packets.
When allow is specified, the peer is allowed to request PFC during LCP negotiation. When deny is specified, the Peer is not allowed to request PFC during LCP negotiation.
transmit { apply | ignore | reject } Default: **ignore**

This keyword specifies how Protocol field Compression should be applied for PPP packets transmitted to the Peer. During LCP negotiation, the Peer indicates whether it can handle PFC compressed PPP packets. When **apply** is specified, if the peer requests PFC, it is accepted and PFC is applied for transmitted PPP packets. When **ignore** is specified, If the peer requests PFC, it is accepted but PFC is not applied for transmitted packets. When **reject** is specified, all requests for PCF from the peer are rejected.

reject-peer-authentication

If disabled, re-enables the system to reject peer requests for authentication. Default: Enabled

renegotiation retain-ip-address

If enabled, retain the currently allocated IP address for the session during PPP renegotiation (Simple IP) between FA and Mobile node. Default: Enabled
If disabled, the initially allocated IP address will be released and a new IP address will be allocated during PPP renegotiation.

retransmit-timeout *milliseconds*

Specifies the number of milliseconds to wait before attempting to retransmit control packets. *milliseconds* must be an integer from 100 through 5000. Default: 3000

Usage

Modify the context PPP options to ensure authentication and communication for PPP sessions have fewer dropped sessions.

Example

The following commands set various PPP options:

```
ppp dormant send-lcp-terminate

ppp max-retransmission 3

ppp peer-authenticate user1 password secretPwd

ppp peer-authenticate user1

ppp retransmit-timeout 1000
```

The following command disables the sending of LCP terminate messages for dormant sessions.

```
no ppp dormant send-lcp-terminate
```

ppp magic-number

Manages magic number checking during LCP Echo message handling. The magic number is a random number chosen to distinguish a peer and detect looped back lines.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] ppp magic-number receive ignore
```

no

Disables the specified behavior.

default

Restores the system defaults for the specific command/keyword.

ppp magic-number receive ignore

Ignores the checking of magic number at the PDSN during LCP Echo message handling. Default: Disabled. If a valid magic numbers were negotiated for the PPP endpoints during LCP negotiation and LCP Echo Request/Response have invalid magic numbers, enabling this command will cause the system to ignore the checking of magic number during LCP Echo message handling.

Usage

Use this command to allow the system to ignore invalid magic number during LCP Echo Request/Response handling.

Example

The following command allows the invalid magic number during LCP Echo Request/Response negotiation:

```
ppp magic-number receive ignore
```

ppp statistics

Changes the manor in which some PPP statistics are calculated.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ppp statistics success-sessions { lcp-max-retry | misc-reasons | remote-terminated
}
```

no

Disable the specified behavior.

ppp statistics success-sessions lcp-max-retry

Alters statistical calculations so that: ppp successful session = successful sessions + lcp-max-retry.

ppp statistics success-sessions misc-reasons

Alters statistical calculations so that: ppp successful session = successful sessions + misc-reasons.

ppp statistics success-sessions remote-terminated

Alters statistical calculations so that: ppp successful session = successful sessions + remote-terminated.

Usage

Use this command to alter how certain PPP statistics are calculated.

Caution: This command alters the way that some PPP statistics are calculated. Please consult your designated service representative before using this command

Example

The following command alters the statistic “ppp successful session” so that it displays the sum of successful sessions and lcp-max-retry:

```
ppp statistics success-sessions lcp-max-retry
```

The following command disables the alteration of the statistic ppp successful session:

```
no ppp statistics success-sessions lcp-max-retry
```

proxy-dns intercept-list

Enters the HA Proxy DNS Configuration Mode and defines a name of a redirect rules list for the domain name servers associated with a particular FA (Foreign Agent) or group of FAs.

Important: HA Proxy DNS Intercept is a license-enabled feature.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

`[ no ] proxy-dns intercept-list` *`name`*

`no`

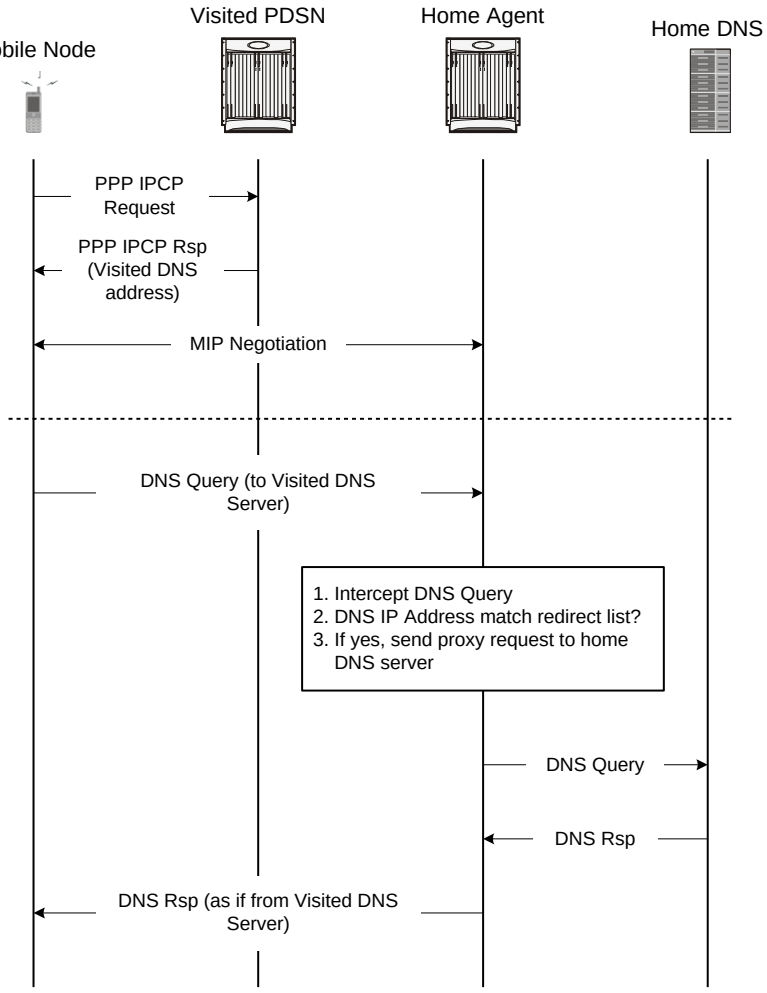
Removes the intercept list from the system.

`proxy-dns intercept-list` *`name`*

Defines the rules list and enters the Proxy DNS Configuration Mode. *`name`* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define a name for a list of rules pertaining to the IP addresses associated with the foreign network's DNS. Up to 128 rules of any type can be configured per rules list.
Upon entering the command, the system switches to the HA Proxy DNS Configuration Mode where the lists can be defines. Up to 64 separate rules lists can be configured in a single AAA context.
This command and the commands in the HA Proxy DNS Configuration Mode provide a solution to the Mobile IP problem that occurs when a MIP subscriber, with a legacy MN or MN that does not support IS-835D, receives a DNS server address from a foreign network that is unreachable from the home network. The following flow shows the steps that occur when this feature is enabled:



By configuring the Proxy DNS feature on the Home Agent, the foreign DNS address is intercepted and replaced with a home DNS address while the call is being handled by the home network.

Example

The following command creates a proxy DNS rules list named *list1* and places the CLI in the HA Proxy DNS Configuration Mode:

```
proxy-dns intercept-list list1
```

radius accounting

This command configures RADIUS accounting parameters for the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius accounting { archive [stop-only] | deadtime *dead_minutes* **| detect-dead-server { consecutive-failures** *consecutive_failures* **| keepalive | response-timeout** *timeout_duration* **} | interim interval** *seconds* **| max-outstanding** *max_messages* **| max-pdu-size** *octets* **| max-retries** *max_retries* **| max-transmissions** *max_transmissions* **| timeout** *timeout_duration* **| unestablished-sessions }**

no radius accounting { archive | detect-dead-server | interim interval | max-transmissions | unestablished-sessions }

default radius accounting { deadtime | detect-dead-server | interim interval *seconds* **| max-outstanding | max-pdu-size | max-retries | max-transmissions | timeout }**

---

no

Removes earlier configuration for the specified keyword.

---

default

Configures the default settings.

---

archive [stop-only]

Enables archiving of RADIUS Accounting messages in the system after the accounting message has exhausted retries to all available RADIUS Accounting servers. All RADIUS Accounting messages generated by a session are delivered to the RADIUS Accounting server in serial. That is, previous RADIUS Accounting messages from the same call must be delivered and acknowledged by the RADIUS Accounting server before the next RADIUS Accounting message is sent to the RADIUS Accounting server.
stop-only specifies archiving of STOP accounting messages only.
Default: Enabled

---

deadtime *dead_minutes*

Specifies the number of minutes to wait before attempting to communicate with a server which has been marked as unreachable.
dead_minutes must be an integer from 0 through 65535.
Default: 10

---

detect-dead-server { consecutive-failures *consecutive_failures* **| keepalive | response-timeout** *timeout_duration* **}**

- **consecutive-failures** *consecutive_failures*: Specifies the number of consecutive failures, for each AAA manager, before a server is marked as unreachable.

consecutive_failures must be an integer from 0 through 1000.

Default: 4

- **keepalive**: Enables the AAA server alive-dead detect mechanism based on sending keepalive authentication messages to all authentication servers.

  Default: Disabled

- **response-timeout** *timeout_duration*: Specifies the number of seconds for each AAA manager to wait for a response to any message before a server is detected as failed, or in a down state.

  timeout_duration must be an integer from 1 through 65535.

Important: If both **consecutive-failures** and **response-timeout** are configured, then both parameters have to be met before a server is considered unreachable, or dead.

interim interval *seconds*

Specifies the time interval (in seconds) for sending accounting INTERIM-UPDATE records. *seconds* must be an integer from 50 through 40000000.

Important: If RADIUS is used as the accounting protocol for the GGSN product, other commands are used to trigger periodic accounting updates. However, these commands would cause RADIUS STOP/START packets to be sent as opposed to INTERIM-UPDATE packets. Also note that accounting interim interval settings received from a RADIUS server take precedence over those configured on the system.

Default: Disabled

max-outstanding *max_messages*

Specifies the maximum number of outstanding messages a single AAA manager instance will queue. *max_messages* must be an integer from 1 through 4000. Default: 256

max-pdu-size *octets*

Specifies the maximum sized packet data unit which can be accepted/generated in bytes (octets). *octets* must be an integer from 512 through 4096. Default: 4096

max-retries *max_retries*

Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as unreachable and the detect dead servers consecutive failures count is incremented. *max_retries* must be an integer from 0 through 65535. Default: 5
Once the maximum number of retries is reached this is considered a single failure for the consecutive failures count for detecting dead servers.

max-transmissions *max_transmissions*

Sets the maximum number of transmissions for a RADIUS accounting message before the message is declared as failed. *max_transmissions* must be an integer from 1 through 65535. Default: Disabled

timeout *seconds*

Specifies the amount of time to wait for a response from a RADIUS server before retransmitting a request. *seconds* must be an integer from 1 through 65535. Default: 3

unestablished-sessions

Indicates RADIUS STOP events are to be generated for sessions that were initiated but never fully established.

Usage

Manage the RADIUS accounting options according to the RADIUS server used for the context.

Example

The following commands configure accounting options.

```
radius accounting detect-dead-server consecutive-failures 5

radius accounting max-pdu-size 1024

radius accounting timeout 16
```

radius accounting algorithm

This command specifies the fail-over/load-balancing algorithm to select the RADIUS accounting server(s) to which accounting data must be sent.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
radius accounting algorithm { first-n n | first-server | round-robin }

default radius accounting algorithm
```

default

Configures the default setting.
Default: **first-server**

first-n *n*

Specifies that the AGW must send accounting data to *n* (more than one) AAA servers based on their priority. The full set of accounting data is sent to each of the *n* AAA servers. Response from any one of the servers would suffice to proceed with the call. On receiving an ACK from any one of the servers, all retries are stopped.
n is the number of AAA servers to which accounting data will be sent, and must be an integer from 2 through 128. Default: 1 (Disabled)

first-server

Specifies that the context must send accounting data to the RADIUS server with the highest configured priority. In the event that this server becomes unreachable, accounting data is sent to the server with the next-highest configured priority. This is the default algorithm.

round-robin

Specifies that the context must load balance sending accounting data among all of the defined RADIUS servers. Accounting data is sent in a circular queue fashion on a per Session Manager task basis, where data is sent to the next available server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.

Usage

Use this command to specify the algorithm to select the RADIUS accounting server(s) to which accounting data must be sent.

Example

The following command specifies to use the round-robin algorithm to select the RADIUS server:

```
radius accounting algorithm round-robin
```

radius accounting apn-to-be-included

This command configures the Access Point Name (APN) to be included for RADIUS accounting.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
radius accounting apn-to-be-included { gi | gn }

default radius accounting apn-to-be-included
```

default

Configures the default setting.

gi

Specifies the usage of the Gi APN name in the RADIUS accounting request. The Gi APN represents the APN received in the Create PDP context request message from the SGSN.

gn

Specifies the usage of the Gn APN name in the RADIUS accounting request. The Gn APN represents the APN selected by the GGSN.

Usage

Use this command to configure the APN name for RADIUS Accounting. This can be set to either gi or gn.

Example

The following command specifies the usage of Gn APN name in the RADIUS accounting request:

```
radius accounting apn-to-be-included gn
```

radius accounting billing-version

This command configures the billing-system version of RADIUS accounting servers.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius accounting billing-version *version*

default radius accounting billing-version

default

Configures the default setting. Default: 0

version

Specifies the billing-system version of RADIUS accounting servers as an integer from 0 through 4294967295. Default: 0

Usage

Use this command to configure the billing-system version of RADIUS accounting servers.

Example

The following command configures the billing-system version of RADIUS accounting servers as *10*:

```
radius accounting billing-version 10
```

radius accounting gtp trigger-policy

This command configures the RADIUS accounting trigger policy for GTP messages.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
radius accounting gtp trigger-policy [ standard | ggsn-preservation-mode ]

default radius accounting gtp trigger-policy
```

default

Resets the RADIUS accounting trigger policy to standard behavior for GTP session.

standard

Sets the RADIUS accounting trigger policy to standard behavior which is configured for GTP session for GGSN service.

ggsn-preservation-mode

Sends RADIUS Accounting Start when the GTP message with private extension of preservation mode is received from SGSN.

Important: This is a customer-specific keyword and needs customer-specific license to use this feature. For more information on GGSN preservation mode, refer to *GGSN Service Configuration Mode Commands* chapter.

Usage

Use this command to set the trigger policy for the AAA accounting for a GTP session.

Example

The following command sets the RADIUS accounting trigger policy for GTP session to standard:

```
default radius accounting gtp trigger-policy
```

radius accounting ha policy

This command configures the RADIUS accounting policy for HA sessions.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
radius accounting ha policy { session-start-stop | custom1-aaa-res-mgmt }

default radius accounting ha policy
```

session-start-stop

Specifies to send Accounting Start when the session is connected, and send Accounting Stop when the session is disconnected. This is the default behavior.

custom1-aaa-res-mgmt

Accounting Start/Stop messages are generated to assist special resource management done by AAA servers. It is similar to the session-start-stop accounting policy, except for the following differences:

- Accounting Start is generated when a new call overwrites an existing session. Accounting Start is also generated during MIP session handoffs.
- No Accounting stop is generated when an existing session is overwritten and the new session continues to use the IP address assigned for the old session.

Usage

Use this command to set the behavior of the AAA accounting for an HA session.

Example

The following command sets the HA accounting policy to **custom1-aaa-res-mgmt**:

```
radius accounting ha policy custom1-aaa-res-mgmt
```

radius accounting interim volume

This command configures the volume of uplink and downlink volume octet counts that triggers RADIUS interim accounting.

Product

GGSN, PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

radius accounting interim volume { downlink *bytes* **uplink** *bytes* **| total** *bytes* **| uplink** *bytes* **downlink** *bytes* **}**

no radius accounting interim volume

no

Disables volume based RADIUS accounting.

downlink *bytes* **uplink** *bytes*

Specifies the downlink to uplink volume limit for RADIUS Interim accounting, in bytes. *bytes* must be an integer to 100000 through 4000000000.

total *bytes*

Specifies the total volume limit for RADIUS interim accounting in bytes. *bytes* must be an integer from 100000 through 4000000000.

uplink *bytes*

Specifies the uplink volume limit for RADIUS interim accounting in bytes. *bytes* must be an integer from 100000 through 4000000000.

downlink *bytes*

Specifies the downlink volume limit for RADIUS interim accounting in bytes. *bytes* must be an integer from 100000 through 4000000000.

Usage

Use this command to trigger RADIUS interim accounting based on the volume of uplink and downlink bytes.

Example

The following command triggers RADIUS interim accounting when the total volume of uplink and downlink bytes reaches *110000*:

```
radius accounting interim volume total 110000
```

radius accounting ip remote-address

This command configures IP remote address-based RADIUS accounting parameters.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

`[ no ] radius accounting ip remote-address { collection | list` *`list_id`* **`}`**

`no`

Removes earlier configuration for the specified keyword.

`collection`

Enables collecting and reporting Remote-Address-Based accounting in RADIUS Accounting. This should be enabled in the AAA Context. It is disabled by default.

`list` *`list_id`*

Enters the Remote Address List Configuration Mode. This mode configures a list of remote addresses that can be referenced by the subscriber's profile. *`list_id`* must be an integer from 1 through 65535.

Usage

This command is used as part of the Remote Address-based Accounting feature to both configure remote IP address lists and enable the collection of accounting data for the addresses in those lists on a per-subscriber basis.

Individual subscriber can be associated to remote IP address lists through the configuration/specification of an attribute in their local or RADIUS profile. (Refer to the **`radius accounting`** command in the Subscriber Configuration mode.) When configured/specified, accounting data is collected pertaining to the subscriber's communication with any of the remote addresses specified in the list.

Once this functionality is configured on the system and in the subscriber profiles, it must be enabled by executing this command with the collection keyword.

Example

The following command enables collecting and reporting Remote-Address-Based accounting in RADIUS Accounting:

```
radius accounting ip remote-address collection
```

radius accounting keepalive

This command configures the keepalive authentication parameters for the RADIUS accounting server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius accounting keepalive { calling-station-id *id* **| consecutive-response** *responses_no_of* **| framed-ip-address** *ip_address* **| interval** *interval_duration* **| retries** *retries_no_of* **| timeout** *timeout_duration* **| username** *user_name* **}**

no radius accounting keepalive framed-ip-address

default radius accounting keepalive { calling-station-id | consecutive-response | interval | retries | timeout | username }

no

Removes configuration for the specified keyword.

default

Configures the default settings.

calling-station-id *id*

Configures the Calling-Station ID to be used for the keepalive authentication as an alphanumeric string of size 1 to 15 characters. Default: 000000000000000

consecutive-response *responses_no_of*

Configures the number of consecutive authentication response after which the server is marked as reachable. *responses_no_of* must be an integer from 1 through 5. Default: 1

framed-ip-address *ip_address*

Specifies the framed ip-address to be used for the keepalive accounting in IPv4 dotted-decimal notation.

interval *interval_duration*

Configures the time interval (in seconds) between the two keepalive access requests. Default: 30

retries *retries_no_of*

Configures the number of times the keepalive access request to be sent before marking the server as unreachable. *retries_no_of* must be an integer from 3 through 10. Default: 3

timeout *timeout_duration*

Configures the time interval between each keepalive access request retries. *timeout_duration* must be an integer from 1 through 30. Default: 3

username *user_name*

Configures the user name to be used for the authentication as an alphanumeric string of 1 through 127 characters. Default: Test-Username

Usage

Configures the keepalive authentication parameters for the RADIUS accounting server.

Example

The following command sets the user name for the RADIUS keepalive access requests to *Test-Username2*:

```
radius accounting keepalive username Test-Username2
```

The following command sets the number of retries to *4*:

```
radius accounting keepalive retries 4
```

radius accounting rp

This command configures the current context's RADIUS accounting R-P originated call options.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
radius accounting rp { handoff-stop { immediate | wait-active-stop } | tod minute hour |
trigger-event { active-handoff | active-start-param-change | active-stop } | trigger-
policy { airlink-usage [ counter-rollover ] | custom [ active-handoff | active-start-
param-change | active-stop ] | standard } | trigger-stop-start }

no radius accounting rp { tod minute hour | trigger-event { active-handoff | active-
start-param-change | active-stop } | trigger-stop-start }

default radius accounting rp { handoff-stop | trigger-policy }
```

no

Removes earlier configuration for the specified keyword.

default

Configures this command with the default settings.

handoff-stop { immediate | wait-active-stop }

Specifies the behavior of generating accounting STOP when handoff occurs.

- **immediate**: Indicates that accounting STOP should be generated immediately on handoff, i.e. not to wait active-stop from the old PCF.
- **wait-active-stop**: Indicates that accounting STOP is generated only when active-stop received from the old PCF when handoff occurs.

Default: **wait-active-stop**

tod *minute hour*

Specifies the time of day a RADIUS event is to be generated for accounting. Up to four different times of the day may be specified through separate commands.
minute must be an integer from 0 through 59.
hour must be an integer from 0 through 23.

trigger-event { active-handoff | active-start-param-change | active-stop }

Configures the events for which a RADIUS event is generated for accounting as one of the following:

- **active-handoff**: Disables a single R-P event (and therefore a RADIUS accounting event) when an Active PCF-to-PFC Handoff occurs. Instead, two R-P events occur (one for the Connection Setup, and the second for the Active-Start). Default: Disabled

- **active-start-param-change**: Disables an R-P event (and therefore a RADIUS accounting event) when an Active-Start is received from the PCF and there has been a parameter change. Default: Enabled
- **active-stop**: Disables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF. Default: Disabled

Important: This keyword has been obsoleted by the **trigger-policy** keyword. Note that if this command is used, if the context configuration is displayed, RADIUS accounting RP configuration is represented in terms of the trigger-policy.

trigger-policy { airlink-usage [counter-rollover] | custom [active-handoff | active-start-param-change | active-stop] | standard }

Default:**airlink-usage**: Disabled
custom:

- **active-handoff**: Disabled
- **active-start-param-change**: Disabled
- **active-stop**: Disabled
- **standard**: Enabled

Configures the overall accounting policy for R-P sessions as one of the following:

- **airlink-usage [counter-rollover]**: Designates the use of Airlink-Usage RADIUS accounting policy for R-P, which generates a start on Active-Starts, and a stop on Active-Stops.

If the **counter-rollover** option is enabled, the system generates a STOP/START pair before input/output data octet counts (or input/output data packet counts) become larger than (2^32 - 1) in value. This setting is used to guarantee that a 32-bit octet count in any STOP message has not wrapped to larger than 2^32 thus ensuring the accuracy of the count. The system, may send the STOP/START pair at any time, so long as it does so before the 32-bit counter has wrapped. Note that a STOP/START pair is never generated unless the subscriber RP session is in the Active state, since octet/packet counts are not accumulated in the Dormant state.

- **custom**: Specifies the use of custom RADIUS accounting policy for R-P. The custom policy can consist of the following:
- **active-handoff**: Enables a single R-P event (and therefore a RADIUS accounting event) when an Active PCF-to-PFC Handoff occurs. Normally two R-P events will occur (one for the Connection Setup, and the second for the Active-Start).
- **active-start-param-change**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Start is received from the PCF and there has been a parameter change.

Important: Note that a custom trigger policy with only **active-start-param-change** enabled is identical to the **standard** trigger-policy.

- **active-stop**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF.

Important: If the **radius accounting rp trigger-policy custom** command is executed without any of the optional keywords, all custom options are disabled.

- **standard**: Specifies the use of Standard RADIUS accounting policy for R-P in accordance with IS-835B.

trigger-stop-start

Specifies that a stop/start RADIUS accounting pair should be sent to the RADIUS server when an applicable R-P event occurs.

Usage

Use this command to configure the events for which a RADIUS event is sent to the server when the accounting procedures vary between servers.

Example

The following command enables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF:

```
radius accounting rp trigger-event active-stop
```

The following command generates the STOP only when active-stop received from the old PCF when handoff occurs:

```
default radius accounting rp handoff-stop
```

radius accounting server

This command configures RADIUS accounting server(s) in the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
radius [ mediation-device ] accounting server ip_address [ encrypted ] key value [ acct-
on { enable | disable } ] [ acct-off { enable | disable } ] [ max max_messages ] [
oldports ] [ port port_number ] [ priority priority ] [ type { mediation-device |
standard } ] [ admin-status { enable | disable } ] [ -noconfirm ]

no radius [ mediation-device ] accounting server ip_address [ oldports | port port_number
]
```

no

Removes the server or server port(s) specified from the list of configured servers.

mediation-device

Enables mediation-device specific AAA transactions use to communicate with this RADIUS server.

Important: If this option is not used, the system by default enables standard AAA transactions.

ip_address

Specifies the IP address of the accounting server.
ip_address must be specified in IPv4 dotted-decimal or IPv6 colon-separated notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

[encrypted] key *value*

Specifies the shared secret key used to authenticate the client to the servers. The **encrypted** keyword indicates the key specified is encrypted.
In 12.1 and earlier releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.
In 12.2 and later releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.
The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **key** keyword is the encrypted version of the plaint text key. Only the encrypted key is saved as part of the configuration file.

acct-on { enable | disable }

Enables and disables sending of the Accounting-On message when a new RADIUS server is added to the configuration.

When enabled, the Accounting-On message is sent when a new RADIUS server is added in the configuration. However, if for some reason the Accounting-On message cannot be sent at the time of server configuration (for example, if the interface is down), then the message is sent as soon as possible. Once the Accounting-On message is sent, if it is not responded to after the configured RADIUS accounting timeout, the message is retried the configured number of RADIUS accounting retries. Once all retries have been exhausted, the system no longer attempts to send the Accounting-On message for this server.
Default: **disable**

---

acct-off { enable | disable }

Default: **enable**
Disables and enables the sending of the Accounting-Off message when a RADIUS server is removed from the configuration.
The Accounting-Off message is sent when a RADIUS server is removed from the configuration, or when there is an orderly shutdown. However, if for some reason the Accounting-On message cannot be sent at this time, it is never sent. The Accounting-Off message is sent only once, regardless of how many accounting retries are enabled.

---

max *max_messages*

Specifies the maximum number of outstanding messages that may be allowed to the server. *max_messages* must be an integer from 1 through 256. Default: 0

---

oldports

Sets the UDP communication port to the out of date standardized default for RADIUS communications to 1646.

---

port *port_number*

Specifies the port number to use for communications as an integer from 1 through 65535. Default: 1813

---

priority *priority*

Specifies the relative priority of this accounting server. The priority is used in server selection for determining which server to send accounting data to.
priority must be an integer from 1 through 1000, where 1 is the highest priority. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the **-noconfirm** option, you are not asked for confirmation and multiple servers could be assigned the same priority.
Default: 1000

---

type { mediation-device | standard }

Specifies the type of AAA transactions to use to communicate with this RADIUS server.

- **standard**: Use standard AAA transactions.
- **mediation-device**: This keyword is obsolete.

Default: **standard**

---

admin-status { enable | disable }

Enables or disables the RADIUS authentication/accounting/ charging server functionality, and saves the status setting in the configuration file to re-establish the set status at reboot.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

This command is used to configure the RADIUS accounting servers with which the system is to communicate for accounting.
Up to 128 RADIUS servers can be configured per context. The servers can be configured as Accounting, Authentication, charging servers, or any combination thereof.

Example

The following commands configure the RADIUS accounting server with the IP address set to 10.2.3.4, port to 1024, and priority to 10:

```
radius accounting server 10.2.3.4 key sharedKey port 1024 max 127

radius accounting server 10.2.3.4 encrypted key scrambledKey oldports
priority 10

no radius accounting server 10.2.5.6
```

The following command sets the accounting server with mediation device transaction for AAA server *10.2.3.4*:

```
radius mediation-device accounting server 10.2.3.4 key sharedKey port
1024 max 127
```

radius algorithm

This command configures the RADIUS authentication server selection algorithm for the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
radius algorithm { first-server | round-robin }

default radius algorithm
```

default

Configures this command with the default setting. Default: **first-server**

first-server

Sends authentication data to the first available server based upon the relative priority of each configured server.

round-robin

Sends authentication data in a circular queue fashion on a per Session Manager task basis where data is sent to the next available server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configure relative priority of the servers.

Usage

Use this command to configure the context's RADIUS server selection algorithm to ensure proper load distribution through the available servers.

Example

The following command configures to use the round-robin algorithm for RADIUS server selection:

```
radius algorithm round-robin
```

radius allow

This command configures the system behavior to allow subscriber sessions when RADIUS accounting and/or authentication is unavailable.

Product

All products used in CDMA deployments

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] radius allow { accounting-down | authentication-down }
```

no

Removes earlier configuration for the specified keyword.

accounting-down

Allows sessions while accounting is unavailable (down). Default: Enabled

authentication-down

Allows sessions while authentication is not available (down). Default: Disabled

Usage

Allow sessions during system troubles when the risk of IP address and/or subscriber spoofing is minimal. The denial of sessions may cause dissatisfaction with subscribers at the cost/expense of verification and/or accounting data.

Important: Please note that this command is applicable ONLY to CDMA products. To configure this functionality in UMTS/LTE products (GGSN/P-GW), use the command **mediation-device delay-GTP-response** in APN Configuration mode.

Example

The following command configures the RADIUS server to allow the sessions while accounting is unavailable:

```
radius allow accounting-down
```

radius attribute

This command configures the system's RADIUS identification parameters.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius attribute { nas-identifier id | nas-ip-address address *primary_address* **[backup** *secondary_address* **] [nexthop-forwarding-address** *nexthop_ip_address* **] [vlan** *vlan_id* **] [mpls-label input** *in_label_value* **output** *out_label_value1 out_label_value1* **] }**

no radius attribute { nas-identifier | nas-ip-address }

default radius attribute nas-identifier

---

no

Removes earlier configuration for the specified keyword.

---

default

Configures the default setting.

---

nas-identifier *id*

Specifies the attribute name by which the system will be identified in Access-Request messages. *id* must be a alphanumeric string of 1 through 32 characters that is case sensitive.

---

nas-ip-address address *primary_address*

Specifies the AAA interface IP address(es) to used to identify the system. Up to two addresses can be configured. *primary_address* is the IP address of the primary interface to use in the current context in IPV4 dotted-decimal or IPv6 colon-separated notation.

---

backup *secondary_address*

Specifies the IP address of the secondary interface to use in the current context in IPV4 dotted-decimal or IPv6 colon-separated notation.

---

mpls-label input *in_label_value* **| output** *out_label_value1* **[** *out_label_value2* **]**

This command configures the traffic from the specified AAA client NAS IP address to use the specified MPLS labels.

- *in_label_value* is the MPLS label that identifies inbound traffic destined for the configured NAS IP address.
- *out_label_value1* and *out_label_value2* identify the MPLS labels to be added to the packets sent from the specified NAS IP address.
  - *out_label_value1* is the inner output label.
  - *out_label_value2* is the outer output label.

MPLS label values must be an integer from 16 through 1048575.

Important: This option is available only when nexthop-forwarding gateway is also configured with the **nexthop-forwarding-address** keyword.

nexthop-forwarding-address *nexthop_ip_address*

Configures the next hop IP address for this NAS IP address in IPV4 dotted-decimal or IPv6 colon-separated notation.

vlan *vlan_id*

Specifies the VLAN ID to be associated with the next-hop IP address as an integer from 1 through 4094.

Usage

This is necessary for NetWare Access Server usage such as the system must be identified to the NAS.
The system supports the concept of the active nas-ip-address. The active nas-ip-address is defined as the current source ip address for RADIUS messages being used by the system. This is the content of the nas-ip-address attribute in each RADIUS message.
The system will always have exactly one active nas-ip-address. The active nas-ip-address will start as the primary nas-ip-address. However, the active nas-ip-address may switch from the primary to the backup, or the backup to the primary. The following events will occur when the active nas-ip-address is switched:

- All current in-process RADIUS accounting messages from the entire system are cancelled. The accounting message is re-sent, with retries preserved, using the ne w active nas-ip-address. Acct-Delay-Time, however, is updated to reflect the time that has occurred since the accounting event. The value of Event-Timestamp is preserved.
- All current in-process RADIUS authentication messages from the entire system are cancelled. The authentication message is re-sent, with retries preserved, using the new active nas-ip-address. The value of Event-Timestamp is preserved.
- All subsequent in-process RADIUS requests uses the new active nas-ip-address.

The system uses a revertive algorithm when transitioning active NAS IP addresses as described below:

- If the configured primary nas-ip-address transitions from UP to DOWN, and the backup nas-ip-address is UP, then the active nas-ip-address switches from the primary to the backup nas-ip-address
- If the backup nas-ip-address is active, and the primary nas-ip-address transitions from DOWN to UP, then the active nas-ip-address switches from the backup to the primary nas-ip-address

Example

The following command configures the RADIUS attribute nas-ip-address as *10.2.3.4*:

```
radius attribute nas-ip-address 10.2.3.4
```

radius authenticate null-username

This command enables (allows) or disables (prevents) the authentication of user names that are blank or empty. This is enabled by default.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] radius authenticate null-username
```

default

Configures the default setting.
Default: Authenticate, send Access-Request messages to the AAA server, all user names, including NULL user names.

no

Disables sending an Access-Request message to the AAA server for user names (NAI) that are blank.

null-username

Enables sending an Access-Request message to the AAA server for user names (NAI) that are blank.

Usage

Use this command to disable, or re-enable, sending Access-Request messages to the AAA server for user names (NAI) that are blank (NULL).

Example

The following command disables sending of Access-Request messages for user names (NAI) that are blank:

```
no radius authenticate null-username
```

The following command re-enables sending of Access-Request messages for user names (NAI) that are blank:

```
radius authenticate null-username
```

radius authenticate apn-to-be-included

This command configures the Access Point Name (APN) to be included for RADIUS authentication.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default ] radius authenticate apn-to-be-included { gi | gn }
```

default

Configures the default setting.

gi

Specifies the use of the Gi APN name in the RADIUS authentication request. The Gi APN represents the APN received in the Create PDP Context Request message from the SGSN.

gn

Specifies the use of the Gn APN name in the RADIUS authentication request. The Gn APN represents the APN selected by the GGSN.

Usage

Use this command to configure the APN name for RADIUS authentication. This can be set to either gi or gn.

Example

The following command specifies the usage of Gn APN name in the RADIUS authentication request.

```
radius authenticate apn-to-be-included gn
```

radius authenticator-validation

This command enables (allows) or disables (prevents) the MD5 authentication of RADIUS users. By default this feature is enabled.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] radius authenticator-validation
```

no

Disables MD5 authentication validation for an Access-Request message to the AAA server.

default

Enables MD5 authentication validation for an Access-Request message to the AAA server.

Usage

Use this command to disable, or re-enable, sending Access-Request messages to the AAA server for MD5 validation.

Example

The following command disables MD5 authentication validation for Access-Request messages for user names (NAI):

```
no radius authenticator-validation
```

The following command enables MD5 authentication validation for Access-Request messages for user names (NAI):

```
radius radius authenticator-validation
```

radius change-authorize-nas-ip

This command configures the NAS IP address and UDP port on which the current context will listen for Change of Authorization (COA) messages and Disconnect Messages (DM). If the NAS IP address is not defined with this command, any COA or DM messages from the RADIUS server are returned with a Destination Unreachable error.

Product

PDSN, FA, HA, GGSN, LNS

Privilege

Security Administrator, Administrator

Syntax

radius change-authorize-nas-ip *ip_address* **[encrypted] key** *value* **[port** *port* **] [event-timestamp-window** *window* **] [no-nas-identification-check] [no-reverse-path-forward-check] [mpls-label input** *in_label_value* **| output** *out_label_value1* **[** *out_label_value2* **]**

no radius change-authorize-nas-ip

no

Deletes the NAS IP address information which disables the system from receiving and responding to COA and DM messages from the RADIUS server.

ip_address

Specifies the NAS IP address of the current context's AAA interface that was defined with the **radius attribute** command.
ip_address can be expressed in IPv4 dotted-decimal or IPv6 colon-separated notation.

[encrypted] key *value*

Specifies the shared secret key used to authenticate the client to the servers. The **encrypted** keyword indicates the key specified is encrypted.
In 12.1 and earlier releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.
In 12.2 and later releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.
The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **key** keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

port *port*

The UDP port on which to listen for CoA and DM messages. Default: 3799

event-timestamp-window *window*

When a COA or DM request is received with an event-time-stamp, if the current-time is greater than the received-pkt-event-time-stamp plus the event-time-stamp-window, the packet is silently discarded
When a COA or DM request is received without the event-timestamp attribute, the packet is silently discarded.

window must be an integer from 0 through 4294967295. If *window* is specified as 0 (zero), this feature is disabled; the event-time-stamp attribute in COA or DM messages is ignored and the event-time-stamp attribute is not included in NAK or ACK messages. Default: 300

no-nas-identification-check

Disables the context from checking the NAS Identifier/ NAS IP Address while receiving the CoA/DM requests. By default this check is enabled.

no-reverse-path-forward-check

Disables the context from checking whether received CoA or DM packets are from one of the AAA servers configured in the current context. Only the src-ip address in the received CoA or DM request is validated and the port and key are ignored. The reverse-path-forward-check is enabled by default.
When reverse-path-forward-check is disabled, CoA and DM messages are accepted from any AAA server.

mpls-label input *in_label_value* **| output** *out_label_value1* **[** *out_label_value2* **]**

This command configures COA traffic to use the specified MPLS labels.

- *in_label_value* is the MPLS label that identifies inbound COA traffic.
- *out_label_value1* and *out_label_value2* identify the MPLS labels to be added to COA response.
  - *out_label_value1* is the inner output label.
  - *out_label_value2* is the outer output label.

MPLS label values must be an integer from 16 through 1048575.

Usage

Use this command to enable the current context to listen for COA and DM messages.
Any one of the following RADIUS attributes may be used to identify the subscriber:

- **3GPP-IMSI**: The subscriber's IMSI. It may include the 3GPP-NSAPI attribute to delete a single PDP context rather than all of the PDP contexts of the subscriber when used with the GGSN product.
- **Framed-IP-address**: The subscriber's IP address.
- **Acct-Session-Id**: Identifies a subscriber session or PDP context.

Important: For the GGSN product, the value for Acct-Session-Id that is mandated by 3GPP is used instead of the special value for Acct-Session-Id that we use in the RADIUS messages we exchange with a RADIUS accounting server.

Important: When this command is used in conjunction with the GGSN, CoA functionality is not supported.

Example

The following command specifies the IP address *192.168.100.10* as the NAS IP address, a key value of *123456* and uses the default port of *3799*:

```
radius change-authorize-nas-ip 192.168.100.10 key 123456
```

The following command disables the nas-identification-check for the above parameters:

```
radius change-authorize-nas-ip 192.168.100.10 key 123456 no-nas-
identification-check
```

radius charging

This command configures basic RADIUS options for Active Charging Services.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius charging { deadtime *dead_minutes* **| detect-dead-server { consecutive-failures** *consecutive_failures* **| response-timeout** *timeout_duration* **} | max-outstanding** *max_messages* **| max-retries** *max_retries* **| max-transmissions** *transmissions* **| timeout** *timeout_duration* **}**

default radius charging { deadtime | detect-dead-server | max-outstanding | max-retries | max-transmissions | timeout }

no radius charging { detect-dead-server | max-transmissions | timeout }

no

Removes configuration for the specified keyword.

default

Configures the default settings.

deadtime *dead_minutes*

Specifies the number of minutes to wait before attempting to communicate with a server which has been marked as unreachable.
dead_minutes must be an integer from 0 through 65535.
Default: 10

detect-dead-server { consecutive-failures *consecutive_failures* **| response-timeout** *timeout_duration* **}**

consecutive-failures *consecutive_failures*: Default: 4. Specifies the number of consecutive failures, for each AAA manager, before a server is marked as unreachable. *consecutive_failures* must be an integer from 0 through 1000.
response-timeout *timeout_duration*: Specifies the number of seconds for each AAA manager to wait for a response to any message before a server is detected as failed, or in a down state. *timeout_duration* must be an integer from 1 through 65535.

max-outstanding *max_messages*

Specifies the maximum number of outstanding messages a single AAA manager instance will queue. *max_messages* must be an integer from 1 through 4000. Default: 256

max-retries *max_retries*

Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as unreachable and the detect dead servers consecutive failures count is incremented. *max_retries* must be an integer from 0 through 65535. Default: 5

max-transmissions *transmissions*

Sets the maximum number of re-transmissions for RADIUS authentication requests. This limit is used in conjunction with the **max-retries** for each server. *transmissions* must be an integer from 1 through 65535. Default: Disabled
When failing to communicate with a RADIUS sever, the subscriber is failed once all of the configured RADIUS servers have been exhausted or once the configured number of maximum transmissions is reached. For example, if 3 servers are configured and if the configured max-retries is 3 and max-transmissions is 12, then the primary server is tried 4 times (once plus 3 retries), the secondary server is tried 4 times, and then a third server is tried 4 times. If there is a fourth server, it is not tried because the maximum number of transmissions (12) has been reached.

timeout *timeout_duration*

Specifies the number of seconds to wait for a response from the RADIUS server before re-sending the messages. *timeout_duration* must be an integer from 1 through 65535. Default: 3

Usage

Manage the basic Charging Service RADIUS options according to the RADIUS server used for the context.

Example

The following command configures the AAA server to be marked as unreachable when the consecutive failure count exceeds 6:

```
radius charging detect-dead-server consecutive-failures 6
```

The following command sets the timeout value to 300 seconds to wait for a response from RADIUS server before resending the messages:

```
radius charging timeout 300
```

radius charging accounting algorithm

This command specifies the fail-over/load-balancing algorithm to be used for selecting RADIUS servers for charging services.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
radius charging accounting algorithm { first-n n | first-server | round-robin }
```

first-n *n*

Specifies that the AGW must send accounting data to *n* (more than one) AAA servers based on their priority. Response from any one of the *n* AAA servers would suffice to proceed with the call. The full set of accounting data is sent to each of the *n* AAA servers.
n is the number of AAA servers to which accounting data will be sent, and must be an integer from 2 through 128. Default: 1 (Disabled)

first-server

Specifies that the context must send accounting data to the RADIUS server with the highest configured priority. In the event that this server becomes unreachable, accounting data is sent to the server with the next-highest configured priority. This is the default algorithm.

round-robin

Specifies that the context must load balance sending accounting data among all of the defined RADIUS servers. Accounting data is sent in a circular queue fashion on a per Session Manager task basis, where data is sent to the next available server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.

Usage

Use this command to specify the accounting algorithm to use to select RADIUS servers for charging services configured in the current context.

Example

The following command specifies to use the round-robin algorithm to select the RADIUS server:

```
radius charging accounting algorithm round-robin
```

radius charging accounting server

This command configures RADIUS charging accounting servers in the current context for Active Charging Services prepaid accounting.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius charging accounting server *ip_address* **[encrypted] key** *key* **[max** *max_messages* **] [max-rate** *max_rate* **] [oldports] [port** *port_number* **] [priority** *priority* **] [admin-status { enable | disable }] [-noconfirm]**

no radius charging accounting server *ip_address* **[oldports | port** *port_number* **]**

---

no

Removes the server or server port(s) specified from the list of configured servers.

---

ip_address

Specifies IP address of the accounting server. in IPv4 dotted-decimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

[encrypted] key *key*

Specifies the shared secret key used to authenticate the client to the servers. The **encrypted** keyword indicates the key specified is encrypted.
In 12.1 and earlier releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.
In 12.2 and later releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.
The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **key** keyword is the encrypted version of the plaint text key. Only the encrypted key is saved as part of the configuration file.

---

max *max_messages*

Specifies the maximum number of outstanding messages that may be allowed to the server. *max_messages* must be integer from 0 through 4000. Default: 0

---

max-rate *max_rate*

Specifies the rate (number of messages per second) at which the authentication messages should be sent to the RADIUS server. *max_rate* must be an integer from 0 through 1000. Default: 0 (Disabled)

---

oldports

Sets the UDP communication port to the out of date standardized default for RADIUS communications to 1646.

port *port_number*

Specifies the port number to use for communications as an integer from 1 through 65535. Default: 1813

priority *priority*

Specifies the relative priority of this accounting server. The priority is used in server selection for determining to which server to send accounting data. *priority* must be an integer 1 through 1000 where 1 is the highest priority. Default: 1000

admin-status { enable | disable }

Enables or disables the RADIUS authentication/ accounting/charging server functionality, and saves the status setting in the configuration file to re-establish the set status at reboot.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

This command is used to configure the RADIUS charging accounting server(s) with which the system is to communicate for Active Charging Services prepaid accounting requests.
Up to 128 AAA servers can be configured per context when the system is functioning as a PDSN and/or HA. Up to 16 servers are supported per context when the system is functioning as a GGSN.

Example

The following commands configure RADIUS charging accounting server with the IP address set to 10.2.3.4, port to 1024, and priority to 10:

```
radius charging accounting server 10.2.3.4 key sharedKey port 1024 max
127

radius charging accounting server 10.2.3.4 encrypted key scrambledKey
oldports priority 10
```

radius charging algorithm

This command configures the RADIUS authentication server selection algorithm for Active Charging Services for the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
radius charging algorithm { first-server | round-robin }

default radius charging algorithm
```

default

Configures the default setting. Default: **first-server**

first-server

Sends accounting data to the first available server based upon the relative priority of each configured server.

round-robin

Sends accounting data in a circular queue fashion on a per Session Manager task basis where data is sent to the next available server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.

Usage

Set the context's RADIUS server selection algorithm for Active Charging Services to ensure proper load distribution through the servers available.

Example

The following command configures to use the round-robin algorithm for RADIUS server selection:

```
radius charging algorithm round-robin
```

radius charging server

This command configures the RADIUS charging server(s) in the current context for Active Charging Services prepaid authentication.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius charging server *ip_address* **[encrypted] key** *key* **[max** *max_messages* **] [max-rate** *max_rate* **] [oldports] [port** *port_number* **] [priority** *priority* **] [admin-status { enable | disable }] [-noconfirm]**

no radius charging server *ip_address* **[oldports | port** *port_number* **]**

---

no

Removes the server or server port(s) specified from the list of configured servers.

---

ip_address

Specifies the IP address of the server in IPv4 dotted-decimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

[encrypted] key *key*

Specifies the shared secret key used to authenticate the client to the servers. The **encrypted** keyword indicates the key specified is encrypted.
In 12.1 and earlier releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.
In 12.2 and later releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.
The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **key** keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

---

max *max_messages*

Specifies the maximum number of outstanding messages that may be allowed to the server. *max_messages* must be an integer from 0 through 4000. Default: 256

---

max-rate *max_rate*

Specifies the rate (number of messages per second), at which the authentication messages should be sent to the RADIUS server. *max_rate* must be an integer from 0 through 1000. Default: 0 (Disabled)

---

oldports

Sets the UDP communication port to the old default for RADIUS communications to 1645.

port *port_number*

Specifies the port number to use for communications as an integer from 1 through 65535. Default: 1812

priority *priority*

Specifies the relative priority of this accounting server. The priority is used in server selection for determining to which server to send accounting data. *priority* must be an integer from 1 through 1000 where 1 is the highest priority. Default: 1000

admin-status { enable | disable }

Enables or disables the RADIUS authentication/accounting/charging server functionality and saves the status setting in the configuration file to re-establish the set status at reboot.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

This command is used to configure the RADIUS charging server(s) with which the system is to communicate for Active Charging Services prepaid authentication requests.
Up to 128 AAA servers can be configured per context when the system is functioning as a PDSN and/or HA. Up to 16 servers are supported per context when the system is functioning as a GGSN.

Example

The following commands configure RADIUS charging server with the IP address set to 10.2.3.4, port to 1024, and priority to 10:

```
radius charging server 10.2.3.4 key sharedKey port 1024 max 127

radius charging server 10.2.3.4 encrypted key scrambledKey oldports
priority 10
```

radius deadtime

This command configures the maximum period of time (in minutes) that must elapse between when a context marks a RADIUS server as unreachable and when it can re-attempt to communicate with the server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius deadtime *minutes*

default radius deadtime

default

Configures the default setting.
Default: 10 minutes

minutes

Specifies the number of minutes to wait before changing the state of a RADIUS server from "Down" to "Active". *minutes* must be an integer from 0 through 65535.

Usage

Use this command to configure the basic RADIUS parameters according to the RADIUS server used for the context.

Important: This parameter should be set to allow enough time to remedy the issue that originally caused the server's state to be changed to "Down". After the deadtime timer expires, the system returns the server's state to "Active" regardless of whether or not the issue has been fixed.

Important: For a complete explanation of RADIUS server states, refer to the *RADIUS Server State Behavior* appendix in the *AAA and GTPP Interface Administration and Reference*.

Example

The following command configures the RADIUS deadtime to 100 minutes:

```
radius deadtime 100
```

radius detect-dead-server

This command configures how the system detects a dead RADIUS server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius detect-dead-server { consecutive-failures *consecutive_failures_count* **| keepalive | response-timeout** *timeout_duration* **}**

{ default | no } radius detect-dead-server

no

Removes the configuration.

default

Configures the default setting.

- **consecutive-failures**: Enabled; 4 consecutive failures
- **keepalive**: Disabled
- **response-timeout**: Disabled

consecutive-failures *consecutive_failures_count*

Specifies the consecutive number of times that the system must find the AAA server unreachable for the server to be marked unreachable, that is the server's state is changed from "Active" to "Down".
consecutive_failures_count must be an integer from 1 through 1000. Default: Enabled; 4 consecutive failures

keepalive

Enables the AAA server alive-dead detect mechanism based on sending keepalive authentication messages to all authentication servers. Default: Disabled

response-timeout *timeout_duration*

Specifies the time duration, in seconds, that the system must wait for a response from the AAA server to any message before the server is marked unreachable, that is the server's state is changed from "Active" to "Down".
timeout_duration must be an integer from 1 through 65535. Default: Disabled

Usage

Use this command to configure how the system detects a dead RADIUS server.

Important: If both **consecutive-failures** and **response-timeout** are configured, then both parameters must be met before a server's state is changed to "Down".

Important: The "Active" or "Down" state of a RADIUS server as defined by the system, is based on accessibility and connectivity. For example, if the server is functional but the system has placed it into a "Down" state, it could be the result of a connectivity problem. When a RADIUS server's state is changed to "Down", a trap is sent to the management station and the **deadtime** timer is started.

Example

The following command enables the detect-dead-server consecutive-failures mechanism and configures the consecutive number of failures to *10*:

```
radius detect-dead-server consecutive-failures 10
```

radius dictionary

Configures the RADIUS dictionary.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius dictionary *dictionary*

default radius dictionary

default

Configures the default setting.

dictionary

Specifies which dictionary to use.
dictionary must be one of the following values:

Table 15. RADIUS Dictionary Types

Dictionary	Description
3gpp	This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in 3GPP 32.015.
3gpp2	This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in IS-835.
custom*XX*	These are customized dictionaries. For information on custom dictionaries, please contact your local service representative. *XX* is the integer of the custom dictionary. NOTE: RADIUS dictionary *custom23* should be used in conjunction with Active Charging Service (ACS).
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.
starent	This dictionary consists of all the attributes in the starent-vsa1 dictionary and incorporates additional VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.
starent-835	This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.

Dictionary	Description
starent-vsa1	This dictionary consists not only of the 3gpp2 dictionary, but also includes vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0–255). This is the default dictionary. ***Important:*** In 12.0 and later releases, no new attributes can be added to the **starent-vsa1** dictionary. If there are any new attributes to be added, these can only be added to the **starent** dictionary. For more information, please contact your Cisco account representative.
starent-vsa1-835	This dictionary consists not only of the 3gpp2-835 dictionary, but also includes vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0–255). This is the default dictionary.

Usage

Use this command to configure the RADIUS dictionary.

Example

The following command configures the RADIUS dictionary standard.

```
radius dictionary standard
```

radius group

This command has been deprecated and is replaced by AAA Server Group configurations. See the *AAA Server Group Configuration Mode Commands* chapter.

radius ip vrf

This command associates the specific AAA group (NAS-IP) with a Virtual Routing and Forwarding (VRF) Context instance for BGP/MPLS, GRE, and IPSec tunnel functionality which needs VRF support for RADIUS communication.
By default the VRF is NULL, which means that AAA group is associated with global routing table.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius ip vrf *vrf_name*

no radius ip vrf

no

Disables the configured IP Virtual Routing and Forwarding (VRF) context instance and removes the association between the VRF context instance and the AAA group instance (NAS-IP).
By default this command is disabled, which means the NAS-IP being used is assumed a non-VRF IP and specific AAA group does not have any VRF association.

vrf_name

Specifies the name of a pre-configured VRF context instance. *vrf_name* is the alphanumeric string of a pre-configured VRF context configured in Context Configuration Mode via the **ip vrf** command.

Caution: Any incorrect configuration, such as associating AAA group with wrong VRF instance or removing a VRF instance, will fail the RADIUS communication.

Usage

Use this command to associate/disassociate a pre-configured VRF context for a feature such as BGP/MPLS VPN or GRE, and IPSec tunneling which needs VRF support for RADIUS communication.
By default the VRF is NULL, which means that AAA group (NAS-IP) is associated with global routing table and NAS-IP being used is assumed a non-VRF IP.
This IP VRF feature can be applied to RADIUS communication, which associates the VRF with the AAA group. This command must be configured whenever a VRF IP is used as a NAS-IP in the AAA group or at the Context level for 'default' AAA group.
This is a required configuration as VRF IPs may be overlapping hence AAA needs to know which VRF the configured NAS-IP belongs to. By this support different VRF-based subscribers can communicate with different RADIUS servers using the same, overlapping NAS-IP address, if required across different AAA groups.

Example

The following command associates VRF context instance *ip_vrf1* with specific AAA group (NAS-IP):

```
radius ip vrf ip_vrf1
```

radius keepalive

This command configures the keepalive authentication parameters for the RADIUS server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
radius keepalive [ calling-station-id id | consecutive-response responses_no_of |
encrypted | interval interval_duration | password | retries retries_no_of | timeout
timeout_duration | username user_name | valid-response access-accept [ access-reject ] ]

default radius keepalive { calling-station-id | consecutive-response | interval |
password | retries | timeout | username | valid-response }
```

default

Configures the default setting for the specified parameter.

calling-station-id *id*

Configures the Calling-Station ID to be used for the keepalive authentication. *id* must be an alphanumeric string of size 1 to 15 characters. Default: 000000000000000

consecutive-response *responses_no_of*

Configures the number of consecutive authentication responses after which the server is marked as reachable. *responses_no_of* must be an integer from 1 through 10. Default: 1

encrypted password

Designates use of encryption for the password.
In 12.1 and earlier releases, *password* must be an alphanumeric string of 1 through 63 characters.
In 12.2 and later releases, *password* must be an alphanumeric string of 1 through 132 characters.
Default: Test-Password

interval *interval_duration*

Configures the time interval (in seconds) between two keepalive access requests. *interval_duration* must be an integer from 30 through 65535. Default: 30

password

Configures the password to be used for the authentication as an alphanumeric string of 1 through 63 characters. Default: Test-Password

retries *retries_no_of*

Configures the number of times the keepalive access request are sent before marking the server as unreachable. *retries_no_of* must be an integer from 3 through 10. Default: 3

timeout *timeout_duration*

Configures the time interval (in seconds) between keepalive access request retries. *timeout_duration* must be an integer from 1 through 30. Default: 3

username *user_name*

Configures the user name to be used for authentication as an alphanumeric string of 1 through 127 characters. Default: Test-Username

valid-response access-accept [*access-reject* **]**

Configures the valid response for the authentication request.
If *access-reject* is configured, then both access-accept and access-reject are considered as success for the keepalive authentication request.
If *access-reject* is not configured, then only access-accept is considered as success for the keepalive access request.
Default: **keepalive valid-response access-accept**

Usage

Use this command to configure the Keepalive Authentication parameters for the RADIUS server.

Example

The following command sets the user name for the RADIUS keepalive access requests to *Test-Username2*:

```
radius keepalive username Test-Username2
```

The following command sets the number of retries to *4*:

```
radius keepalive retries 4
```

radius max-outstanding

This command configures the maximum number of outstanding messages a single AAA Manager instance will queue.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius max-outstanding *max_messages*

default radius max-outstanding

default

Configures the default setting.
Default: 256

max_messages

Specifies the maximum number of outstanding messages a single AAA Manager instance will queue. *max_messages* must be an integer from 1 through 4000. Default: 256

Usage

Use this command to configure the maximum number of outstanding messages a single AAA Manager instance will queue.

Example

The following command configures the maximum number of outstanding messages a single AAA Manager instance will queue to *100*:

```
radius max-outstanding 100
```

radius max-retries

This command configures the maximum number of times communication with a AAA server will be attempted before it is marked as “Not Responding”.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius max-retries *max_retries*

default radius max-retries

default

Configures the default setting.

max_retries

Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as “Not Responding”, and the detect dead server’s consecutive failures count is incremented. *max_retries* must be an integer from 0 through 65535. Default: 5

Usage

Use this command to configure the maximum number of times communication with a AAA server will be attempted before it is marked as “Not Responding”.

Example

The following command configures the maximum number of times communication with a AAA server will be attempted before it is marked as “Not Responding” to *10*:

```
radius max-retries 10
```

radius max-transmissions

This command configures the maximum number of re-transmissions for RADIUS authentication requests.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius max-transmissions *max_transmissions*

{ default | no } radius max-transmissions

no

Deletes the RADIUS max-transmissions configuration.

default

Configures the default setting.
Default: Disabled

max_transmissions

Specifies the maximum number of re-transmissions for RADIUS authentication requests. This limit is used in conjunction with **radius max-retries** configuration for each server. *max_transmissions* must be an integer from 1 through 65535. Default: Disabled
When failing to communicate with a RADIUS sever, the subscriber is failed once all of the configured RADIUS servers have been exhausted, or once the configured number of maximum transmissions is reached. For example, if three servers are configured and if the configured max-retries is 3 and max-transmissions is 12, then the primary server is tried four times (once plus three retries), the secondary server is tried four times, and then a third server is tried four times. If there is a fourth server, it is not tried because the maximum number of transmissions (12) has been reached.

Usage

Use this command to configure the maximum number of re-transmissions for RADIUS authentication requests.

Example

The following command configures the maximum number of re-transmissions for RADIUS authentication requests to *10*:

```
radius max-transmissions 10
```

radius mediation-device

See the **radius accounting server** command.

radius probe-interval

This command configures the interval between two RADIUS authentication probes.

Product

All products supporting Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Syntax

radius probe-interval *seconds*

default radius probe-interval

default

Configures the default setting of 3.

seconds

Specifies the time duration (in seconds) to wait before sending another probe authentication request to a RADIUS server. The value must be an integer from 1 through 65535. Default: 3

Usage

Use this command for ICSR support to set the duration between two authentication probes to the RADIUS server.

Example

The following command sets the authentication probe interval to 30 seconds.

```
radius probe-interval 30
```

radius probe-max-retries

This command configures the number of retries for RADIUS authentication probe response.

Product

All products supporting Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Syntax

radius probe-max-retries *retries*

default radius probe-max-retries

default

Configures the default setting.
Default: 5

retries

Specifies the number of retries for RADIUS authentication probe response before the authentication is declared as failed. *retries* must be an integer from 1 through 65535. Default: 5

Usage

Use this command for ICSR support to set the number of attempts to send RADIUS authentication probe without a response before the authentication is declared as failed.

Example

The following command sets the maximum number of retries to *6*:

```
radius probe-max-retries 6
```

radius probe-message

This command configures the service ip-address to be sent as an AVP in RADIUS authentication probe messages.

Product

All products supporting Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Syntax

radius probe-message local-service-address *ipv4/ipv6_address*

no radius probe-message local-service-address

---

no

Disables sending of AVPs configured under probe-message cli in RADIUS authentication probe messages.

---

radius probe-message local-service-address

radius probe-message
Configures AVPs to be sent in RADIUS authentication probe messages.
local-service-address
Configures the service ip-address to be sent as an AVP in RADIUS authentication probe messages.

---

ipv4/ipv6_address

Specifies the IPv4/IPv6 address of the server in IPv4 dotted-decimal or IPv6 colon-separated notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

Example

The following command configures the service ip-address *21.32.36.25* to be sent as an AVP in RADIUS authentication probe messages:

```
radius probe-message local-service-address 21.32.36.25
```

radius probe-timeout

This command configures the timeout duration to wait for a response for RADIUS authentication probes.

Product

All products supporting Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Syntax

radius probe-timeout *timeout_duration*

default radius probe-timeout

default

Configures the default setting.
Default: 3

timeout_duration

Specifies the time duration (in seconds) to wait for a response from the RADIUS server before resending the authentication probe. *timeout_duration* must be an integer from 1 through 65535. Default: 3

Usage

Use this command for ICSR support to set the duration to wait for a response before re-sending the RADIUS authentication probe to the RADIUS server.

Example

The following command sets the authentication probe timeout to *120* seconds:

```
radius probe-timeout 120
```

radius server

This command configures RADIUS authentication server(s) in the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
radius server ip_address [ encrypted ] key value [ max max_messages ] [ max-rate max_rate
] [ oldports ] [ port port_number ] [ priority priority ] [ probe | no-probe ] [ probe-
username user_name ] [ probe-password [ encrypted ] password password ] [ type {
mediation-device | standard } ] [ admin-status { enable | disable } ] [ -noconfirm ]

no radius server ip_address [ oldports | port port_number ]
```

no

Removes the server or server port(s) specified from the list of configured servers.

ip_address

Specifies the IP address of the server in IPv4 dotted-decimal or IPv6 colon-separated notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

[encrypted] key *value*

Specifies the shared secret key used to authenticate the client to the servers. The **encrypted** keyword indicates the key specified is encrypted.
In 12.1 and earlier releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.
In 12.2 and later releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.
The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **key** keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

max *max_messages*

Specifies the maximum number of outstanding messages that may be allowed to the server. *max_messages* must be an integer from 0 through 4000. Default: 256

max-rate *max_rate*

Specifies the rate (number of messages per second), at which the authentication messages should be sent to the RADIUS server. *max_rate* must be an integer from 0 through 1000. Default: 0 (Disabled)

oldports

Sets the UDP communication port to the old default for RADIUS communications to 1645.

port *port_number*

Specifies the port number to use for communications as an integer from 1 through 65535. Default: 1812

priority *priority*

Specifies the relative priority of this accounting server. The priority is used in server selection for determining to which server is to send accounting data.
priority must be an integer from 1 through 1000 where 1 is the highest priority. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the **-noconfirm** option, you are not asked for confirmation and multiple servers could be assigned the same priority.
Default: 1000

probe

Enables probe messages to be sent to the specified RADIUS server.

no-probe

Disables probe messages from being sent to the specified RADIUS server. This is the default behavior.

probe-username *username*

Specifies the user name sent to the RADIUS server to authenticate probe messages. *username*must be an alphanumeric string of 1 through 127 characters.

probe-password [encrypted] password *password*

The password sent to the RADIUS server to authenticate probe messages.
encrypted: This keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.
password *password*: Specifies the probe-user password for authentication. *password* must be an alphanumeric string of 1 through 63 characters.

type { mediation-device | standard }

Specifies the type of transactions the RADIUS server accepts.
mediation-device: Specifies mediation-device specific AAA transactions. This device is available if you purchased a transaction control services license. Contact your local sales representative for licensing information.
standard: Specifies standard AAA transactions. (Default)

admin-status { enable | disable }

Enables or disables the RADIUS authentication/accounting/charging server functionality, and saves the status setting in the configuration file to re-establish the set status at reboot.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

This command is used to configure the RADIUS authentication server(s) with which the system is to communicate for authentication.
Up to 128 RADIUS servers can be configured per context. The servers can be configured as Accounting, Authentication, charging servers, or any combination thereof.

Example

The following commands configure RADIUS server with the IP address set to 10.2.3.4, port to 1024, and priority to 10:

```
radius server 10.2.3.4 key sharedKey port 1024 max 127

radius server 10.2.3.4 encrypted key scrambledKey oldports priority 10
```

radius strip-domain

This command configures the stripping of the domain from the user name prior to authentication or accounting.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
radius strip-domain { authentication-only | accounting-only }

no radius strip-domain
```

no

Removes the RADIUS strip-domain configuration.

authentication-only

Specifies that the domain must be stripped from the user name prior to authentication.

accounting-only

Specifies that the domain must be stripped from the user name prior to accounting.

Usage

Use this command to configure the stripping of domain from the user name prior to authentication or accounting.
By default, strip-domain configuration will be applied to both authentication and accounting messages, if configured. When the argument **authentication-only** or **accounting-only** is present, **strip-domain** is applied only to the specified RADIUS message types.

Example

The following command configures the stripping of domain from the user name prior to authentication:

```
radius strip-domain authentication-only
```

radius timeout

This command configures the time duration to wait for a response from the RADIUS server before resending the messages.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius timeout *timeout_duration*

default radius timeout

default

Configures the default setting.

timeout_duration

Specifies the time duration (in seconds) to wait for a response from the RADIUS server before resending the messages. *timeout_duration* must be an integer from 1 through 65535. Default: 3

Usage

Use this command to configure the time duration to wait for a response from the RADIUS server before resending the messages.

Example

The following command configures the RADIUS timeout parameter to 300 seconds:

```
radius timeout 300
```

radius trigger

This command enables specific RADIUS triggers. The RADIUS Trigger configuration in the Context Configuration Mode is to enable backward compatibility. To configure RADIUS triggers for the default AAA group, you must configure them in the Context Configuration Mode.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] radius trigger { ms-timezone-change | qos-change | rai-change | rat-change |
serving-node-change | uli-change }

default radius trigger
```

no

Disables the specified RADIUS trigger.

default

Configures the default setting.
Default: All RADIUS triggers are enabled.

ms-timezone-change

Specifies to enable RADIUS trigger for MS time zone change.

qos-change

Specifies to enable RADIUS trigger for Quality of Service change.

rai-change

Specifies to enable RADIUS trigger for Routing Area Information change.

rat-change

Specifies to enable RADIUS trigger for Radio Access Technology change.

serving-node-change

Specifies to enable RADIUS trigger for Serving Node change.

uli-change

Specifies to enable RADIUS trigger for User Location Information change.

Usage

Use this command to enable RADIUS triggers.

Example

The following command enables RADIUS trigger for RAT change:

```
radius trigger rat-change
```

route-access-list extended

Configures an access list for filtering routes based on a specified range of IP addresses.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

[no] route-access-list extended *identifier* **{ deny | permit } ip {** *network_parameter* **} {** *mask_parameter*

---

no

Deletes the specified route access list.

---

route-access-list extended *identifier*

Specifies a value to identify the route access list as an integer from 100 through 999.

---

deny

Deny routes that match the specified criteria.

---

permit

Permit routes that match the specified criteria.

---

ip *network_parameter ip_address wildcard_mask*

Specifies the network portion of the route to match. The network portion of the route is mandatory and must be expressed in one of the following ways:

- *ip_address wildcard_mask*: Matches a network address and wildcard mask expressed in IPv4 dotted-decimal notation.
- **any**: Matches any network address.
- **host** *network_address*: Match the specified network address exactly. *network_address* must be an IPv4 address specified in dotted-decimal notation.

---

mask_parameter

This specifies the mask portion of the route to match. The mask portion of the route is mandatory and must be expressed in one of the following ways:

- *mask_address wildcard_mask*: A mask address and wildcard mask expressed in IPv4 dotted-decimal notation.
- **any**: Match any network mask.
- **host** *mask_address*: Match the specified mask address exactly. *mask_address* must be an IPv4 address specified in dotted-decimal notation.

Usage

Use this command to create an extended route-access-list that matches routes based on network addresses and masks.

Example

Use the following command to create an extended route-access-list:

```
route-access-list extended 100 permit ip 192.168.100.0 0.0.0.255
```

route-access-list named

Configures an access list for filtering routes based on a network address and net mask.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

[no] route-access-list named *list_name* **{ deny | permit } {** *ip_address*/*mask* **| any } [exact-match]**

no

Deletes the specified route access list.

route-access-list named *list_name*

Specifies name that identifies the route access list as an alphanumeric string of 1 through 79 characters.

deny

Denies routes that match the specified criteria.

permit

Permits routes that match the specified criteria.

ip_address/*mask*

Specifies the IP address (in IPv4 dotted-decimal notation) and the number of subnet bits, representing the subnet mask in CIDR notation (for example 10.1.1.1/24).

any

Matches any route.

exact-match

Matches the IP address prefix exactly.

Usage

Use this command to create route-access lists that specify routes that are accepted.

Example

Use the following command to create a route access list named *list27* that permits routes that match *192.168.1.0/24* exactly:

```
route-access-list named list 27 permit 192.168.1.0/24 exact-match
```

To delete the list, use the following command:

```
no route-access-list named list 27 permit 192.168.1.0/24 exact-match
```

route-access-list standard

Configures an access-list for filtering routes based on network addresses.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

[no] route-access-list standard *identifier* **{ permit | deny } {** *ip_address wildcard_mask* **| any | host** *network_address* **}**

no

Deletes the specified route access list.

route-access-list standard *identifier*

Specifies a value that identifies the route-access-list as an integer from 1 through 99.

deny

Denies routes that match the specified criteria.

permit

Permits routes that match the specified criteria.

ip_address wildcard_mask

Specifies the IP address and subnet mask to match for routes. Both *ip_address* and *wildcard_mask* must be entered in IPv4 dotted-decimal notation. (For example, 192.168.100.0 255.255.255.0)

any

Matches any route.

host *network_address*

Matches only routes having the specified network address as if it had a 32-bit network mask. *network_address* must be an IPv4 address specified in dotted-decimal notation.

Usage

Use this command to create route-access-lists that specify routes that are accepted.

Example

Use the following command to create a route access list with an identifier of *10* that permits routes:

```
route-access-list standard 10 permit 192.168.1.0 255.255.255.0
```

To delete the list, use the following command:

```
no route-access-list standard 10 permit 192.168.1.0 255.255.255.0
```

route-map

Creates a route-map that is used by the routing features and enters Route-map Configuration mode. A route-map allows redistribution of routes and includes a list of match and set commands associated with it. The match commands specify the conditions under which redistribution is allowed; the set commands specify the particular redistribution actions to be performed if the criteria specified by match commands are met. Route-maps are used for detailed control over route distribution between routing processes. Up to eight route-maps can be created in each context. Refer to the *Route-map Configuration Mode Commands* chapter for more information.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

route-map *map_name* **{ deny | permit }** *seq_number*

no route-map *map_name*

no

Deletes the specified route map.

route-map *map_name*

Specifies the name of the route map to create or edit as an alphanumeric string of 1 through 69 characters.

deny

If the deny parameter is specified and the match command criteria are met, the route is not redistributed and any other route maps with the same map name are not examined. Set commands have no affect on deny route-maps.

permit

If the permit parameter is specified, and the match criteria are met, the route is redistributed as specified by set actions. If the match criteria are not met, the next route map with the same name is tested.

seq_number

Specifies the sequence number that indicates the position a new route map is to have in the list of route maps already configured with the same name. Route maps with the same name are tested in ascending order of their sequence numbers. This must be an integer from 1 through 65535.

Usage

Use this command to create route maps that allow redistribution of routes based on specified criteria and set parameters for the routes that get redistributed. The chassis supports a maximum of 64 route maps per context.

Example

To create a route map named map1 that permits routes that match the specified criteria, use the following command:

```
route-map map1 permit 10
```

To delete the route-map, enter the following command:

```
no route-map map1 permit 10
```

router

Enables BGP, Open Shortest Path First (OSPF) or OSPF version 3 (OSPFv3) routing functionality and enters the corresponding Configuration Mode. Refer to the *BGP Configuration Mode Commands*, *OSPF Configuration Mode Commands* or *OSPFv3 Configuration Mode Commands* chapter for details on associated Configuration mode commands.

Product

PDSN, HA, GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] router { bgp as_number | ospf | ospfv3  }
```

no

Disables the specified routing support in the current context.

bgp *as_number*

Enables a BGP routing service for this context and assigns it the specified Autonomous System (AS) number before entering the BGP Configuration mode. *as_number* must be an integer from 1 through 4294967295.

Important: BGP routing is supported only for use with the HA.

ospf

Enables OSPF routing in this context and enters OSPF Configuration mode.

ospfv3

Enables OSPFv3 routing in this context and enter OSPFv3 Configuration mode.

Usage

Use this command to enable and configure OSPF and BGP routing in the current context.

Important: You must obtain and install a valid license key to use these features. Refer to the *System Administration Guide* for details on obtaining and installing feature use license keys.

Example

The following command enables the OSPF routing functionality and enters the OSPF Configuration Mode:

```
router ospf
```

The following command enables the OSPFv3 routing functionality and enters the OSPFv3 Configuration Mode:

```
router ospfv3
```

The following command enables a BGP routing service with an AS number of *100*, and enters the BGP Configuration Mode:

```
router bgp 100
```

server

Configures remote server access protocols for the current context. This command is used to enter the specified protocols configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
server { ftpd | named | sshd | telnetd | tftpd }

no server { ftpd | named | sshd | telnetd | tftpd } [ kill ]
```

no

Disables the specified service.

server ftpd

Enters the FTP Server Configuration Mode.

Important: The FTPD server can only be configured in the local context.

server named

Starts the named server.

server sshd

Enters the SSH Server Configuration Mode.

Important: The SSHD server allows only three unsuccessful login attempts before closing a login session attempt.

server telnetd

Enters the Telnet Server Configuration Mode.

Important: The TELNET server allows only three unsuccessful login attempts before closing a login session attempt.

server tftpd

Enters the TFTP Server Configuration Mode.

Important: The TFTPD server can only be configured in the local context.

kill

Indicates all instances of the server are to be stopped.
This option only works with the **ftpd**, **sshd**, **telnetd**, and **tftpd** commands.

Usage

Enter the Context Configuration Mode for the appropriate, previously defined context, to set the server option(s). Repeat the command as needed to enable/disable more than one option server daemon.

Example

```
server ftpd

server named

no server tftpd

server sshd

server telnetd

no server telnetd kill
```

service-redundancy-protocol

Configures Interchassis Session Recovery (ICSR) services for the current context. This command is used to enter the Service Redundancy Protocol Configuration Mode.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

```
service-redundancy-protocol
```

Usage

Enter the configuration mode to set the service redundancy protocol options.

Example

The following command enters Service Redundancy Protocol Configuration Mode.

```
service-redundancy-protocol
```

session-event-module

Enables the event module, enters the Session Event Module Configuration Mode where the sending of Serving Gateway (S-GW) subscriber-specific event files to an external server can be configured.

Product

S-GW

Privilege

Administrator

Syntax

```
[ no ] session-event-module
```

no

Disables the event module configuration.

Usage

Enter the Session Event Module Configuration Mode where the sending of S-GW subscriber-specific event files to an external server can be configured.
Entering this command results in the following prompt:

```
[context_name]hostname(config-event)#
```

Session Event Module Configuration Mode commands are defined in the *Session Event Module Configuration Mode Commands* chapter.

sgsn-service

Creates an SGSN service instance and enters the SGSN Service Configuration mode. This mode configures or edits the configuration for an SGSN service which controls the SGSN functionality.

An SGSN mediates access to GPRS/UMTS network resources on behalf of user equipment (UE) and implements the packet scheduling policy between different QoS classes. It is responsible for establishing the packet data protocol (PDP) context with the GGSN.

Important: For details about the commands and parameters, check the *SGSN Service Configuration Mode* chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] sgsn-service *srvc_name*

no

Remove the configuration for the specified SGSN service from the configuration of the current context.

sgsn-service *srvc_name*

Specifies the name of the SGSN service as a unique alphanumeric string of 1 through 63 characters.

Usage

Use this command to create, edit, or remove an SGSN service

Example

The following command creates an SGSN service named *sgsn1* in the current context:

```
sgsn-service sgsn1
```

The following command removes the sgsn service named *sgsn1* from the configuration for the current context:

```
no sgsn-service sgsn1
```

sgs-service

Creates an SGs service instance and enters the SGS Service Configuration mode.

Product

MME

Privilege

Administrator

Syntax

[no] sgs-service *name*

no

Remove the configuration for the specified SGs service from the configuration of the current context.

sgs-service *name*

Specifies a name for an SGs service as a unique alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Enter the SGS Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following CLI prompt:

```
[context_name]hostname(config-sgs-service)#
```

SGS Service Configuration Mode commands are defined in the *SGS Service Configuration Mode Commands* chapter.

Example

The following command creates an SGS service named *sgs1* in the current context:

```
sgs-service sgs1
```

The following command removes the SGS service named *sgs1* from the configuration for the current context:

```
no sgs-service sgs1
```

sgtp-service

Creates an SGTP service instance and enters the SGTP Service Configuration mode. This mode configures the GPRS Tunneling Protocol (GTP) related settings required by the SGSN to support GTP-C (control plane) messaging and GTP-U (user data plane) messaging.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] sgtp-service *svc_name*

no

Remove the configuration for the specified SGTP service from the configuration of the current context.

sgtp-service *svc_name*

Specifies a name for an SGTP service as a unique alphanumeric string of 1 through 63 characters.

Usage

Use this command to create, edit, or remove an SGTP service

Example

The following command creates an SGTP service named *sgtp1* in the current context:

```
sgtp-service sgtp1
```

The following command removes the sgsn service named *sgtp1* from the configuration for the current context:

```
no sgtp-service sgtp1
```

sgw-service

Creates an S-GW service or specifies an existing S-GW service and enters the S-GW Service Configuration Mode for the current context.

Product

S-GW

Privilege

Administrator

Syntax

sgw-service *service_name* **[-noconfirm]**

no sgw-service *service_name*

sgw-service *service_name*

Specifies the name of the S-GW service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no sgw-service *service_name*

Removes the specified S-GW service from the context.

Usage

Enter the S-GW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-sgw-service)#
```

S-GW Service Configuration Mode commands are defined in the *S-GW Service Configuration Mode Commands* chapter.
Use this command when configuring the following SAE components: S-GW.

Example

The following command enters the existing S-GW Service Configuration Mode (or creates it if it does not already exist) for the service named *sgw-service1*:

```
sgw-service sgw-service1
```

The following command will remove *spgw-service1* from the system:

```
no sgw-service sgw-service1
```

ssh

Generates public and private keys for use with the configured Secure Shell (SSH) server for the current context and sets the public/private key pair to specified values.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ssh { generate key | key *data* **length** *octets* **} [type { v1-rsa | v2-rsa | v2-dsa }]**

no ssh key [type { v1-rsa | v2-rsa | v2-dsa }]

no ssh key [type { v1-rsa | v2-rsa | v2-dsa }]

This command clears configured SSH keys. If type is not specified, all SSH keys are cleared.

ssh generate key

Generates a public/private key pair which is to be used by the SSH server. The generated key pair is in use until the command is issued again.

ssh key *data* **length** *octets*

Sets the public/private key pair to be used by the system where *data* is the encrypted key and *length* is the length of the encrypted key in octets. *data* must be an alphanumeric string of 1 through 1023 characters and *octets* must be a value in the range of 0 through 65535.

[type { v1-rsa | v2-rsa | v2-dsa }]

Specifies the type of SSH key to generate. If type is not specified, all three key types are generated.

- **v1-rsa**: SSH v1 RSA host key only
- **v2-rsa**: SSH v2 DSA host key only
- **v2-dsa**: SSH v2 RSA host key only

Important: For maximum security, it is recommended that only SSH v2 be used. **v2-rsa** is the recommended key type.

Usage

Generate secure shell keys for use in public key authentication.

Example

```
ssh generate key

ssh key g6j93fw59cx length 128
```

ssl

Creates a new Secure Sockets Layer (SSL) template or specifies an existing one and enters the SSL Template Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

[no] ssl template *name* **{ ssl-subscriber }**

no

Removes the specified SSL template from the context.

ssl template *name*

Specifies the name of a new or existing SSL template as an alphanumeric string of 1 through 127 alphanumeric characters.

ssl-subscriber

Specifies that the SSL template is an SSL subscriber template.

Usage

Use this command to create a new SSL template or modify an existing one.
Entering this command results in the following prompt:

```
[context_name]hostname(cfg-ctx-ssl-subscriber-template)#
```

SSL Template Configuration Mode commands are defined in the *SSL Template Configuration Mode Commands* chapter.

Example

The following command specifies the SSL template *ssl_template_1* and enters the SSL Template Configuration Mode:

```
ssl template ssl_template_1 ssl-subscriber
```

subscriber

Configures the specified subscriber for the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

subscriber { default | name *user_name* **} asn-service-info mobility [ipv4 | ipv6 | ipv6-ipv4]**

no subscriber { default | name *user_name* **}**

no

Indicates the subscriber specified is to be removed from the list of allowed users for the current context.

subscriber default | name *user_name*

default: Enters the Subscriber Configuration Mode for the context's default subscriber settings.
name *user_name*: Specifies the user which is to be allowed to use the services of the current context. *user_name* must be an alphanumeric string of 1 through 127 characters.
asn-service-info mobility: Indicates the type of mobility supported and enabled in the Autonomous System Number (ASN).

Usage

Enter the Subscriber Configuration Mode for actual users as well as for a default subscriber for the current context.
NAS uses the specified parameter for asn-service-info mobility to indicate and pack the mobility support field for IPv4, IPv6, or both, in the Service-Info attribute in the Access-request. RADIUS sends back this attribute in the Access-accept message by indicating respective bits to authorize the service indicated by NAS.

Important: A maximum of 128 subscribers and/or administrative users may be locally configured per context.

Example

Following command configures the default subscriber in a context:

```
subscriber default
```

Following command removes the default subscriber from a context:

```
no subscriber default
```

Following command configures a subscriber named *user1* in a context:

```
subscriber name user1
```

Following command removes a subscriber named *user1* from a context:

```
no subscriber name user1
```

threshold available-ip-pool-group

Configures context-level thresholds for IP pool utilization for the system.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold available-ip-pool-group *low_thresh* **[clear** *high_thresh* **]**

default threshold available-ip-pool-group

default

Configures the default setting.

threshold available-ip-pool-group *low_thresh*

The low threshold IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. *low_thresh* can be configured as an integer from 0 through 100. Default: 10

clear *high_thresh*

Specifies the high threshold IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. *high_thresh* can be configured as an integer from 0 through 100. Default: 10

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

When IP address pools are configured on the system, they can be assigned to a group. IP address pool utilization thresholds generate alerts or alarms based on the utilization percentage of all IP address contained in the pool group during the specified polling interval.

All configured public IP address pools that were not assigned to a group are treated as belonging to the same group. Individual configured static or private pools are each treated as their own group.

Alerts or alarms are triggered for IP address pool utilization based on the following rules:

- **Enter Condition**: Actual IP address utilization percentage per pool group ≤ Low Threshold
- **Clear Condition**: Actual IP address utilization percentage per pool group > High Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

The following table describes the possible methods for configuring IP pool utilization thresholds:

Table 16. IP Pool Utilization Thresholds - Configuration Methods

Method	Description
Context-level	A single IP pool utilization threshold can be configured for all IP pool groups within a given system context. If a single threshold is configured for all pool groups, separate alerts or alarms can be generated for each group. This command configures that threshold.
IP address pool-level	Each individual IP address pool can be configured with its own threshold. Thresholds configured for individual pools take precedence over the context-level threshold that would otherwise be applied (if configured). In the event that two IP address pools belonging to the same pool group are configured with different thresholds, the system uses the pool configuration that has the greatest low threshold for that group.

Example

The following command configures a context-level IP pool utilization low threshold percentage of *10* and a high threshold of *35* for an system using the Alarm thresholding model:

```
threshold available-ip-pool-group 10 clear 35
```

threshold ha-service init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for an HA service.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
threshold ha-service init-rrq-rcvd-rate high_thresh [ clear low_thresh ]

no threshold ha-service init-rrq-rcvd-rate
```

no

Deletes the alert or alarm.

threshold ha-service init-rrq-rcvd-rate *high_thresh*

Sets the high threshold average number of calls setup per second that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 1000000. Default: 0

clear *low_thresh*

Sets the low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured as an integer from 0 through 1000000. Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the average number of calls setup per second is equal to or less than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter Condition**: Actual number of calls setup per second > High Threshold
- **Clear Condition**: Actual number of calls setup per second ≤ Low Threshold

Example

The following command configures a number of calls setup per second threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold ha-service init-rrq-rcvd-rate 1000 clear 500
```

threshold ip-pool-free

Sets an alarm or alert based on the percentage of IP addresses that are unassigned in an IP pool. This command affects all IP pools in the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold ip-pool-free *low_thresh* **[clear** *high_thresh* **]**

default threshold ip-pool-free

default

Configures the default setting.

threshold ip-pool-free *low_thresh*

Sets the low threshold percentage of addresses available in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer between 0 and 100. Default: 0

clear *high_thresh*

Sets the high threshold percentage of addresses available in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. It may be configured as an integer between 0 and 100. Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

Use this command to set an alert or an alarm when the number of unassigned IP addresses in any pool is equal to or less than a specified percentage of the total number of addresses in the pool.
Alerts or alarms are triggered for percentage of IP address pool free based on the following rules:

- **Enter Condition**: Actual percentage of IP addresses free per pool ≤ Low Threshold
- **Clear Condition**: Actual percentage of IP addresses free per pool > High Threshold

Important: This command is overridden by the settings of the **alert-threshold** keyword of the **ip pool** command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are unused low threshold percentage of *10* and a high threshold of *35* for an system using the Alarm thresholding model:

```
threshold ip-pool-free 10 clear 35
```

threshold ip-pool-hold

Sets an alert based on the percentage of IP addresses from an IP pool that are on hold. This command affects all IP pools in the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold ip-pool-hold *high_thresh* **[clear** *low_thresh* **]**

default threshold ip-pool-hold

default

Configures the default setting.

threshold ip-pool-hold *high_thresh*

Sets the high threshold percentage of addresses on hold in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 100. Default: 0

clear *low_thresh*

Sets the low threshold percentage of addresses on hold in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises below the low threshold within the polling interval, a clear alarm will be generated. It may be configured as an integer from 0 through 100. Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the percentage of IP addresses on hold in any pool is equal to or greater than a specified percentage of the total number of addresses in the pool.
Alerts or alarms are triggered for percentage of IP address pool addresses on hold based on the following rules:

- **Enter Condition**: Actual percentage of IP addresses on hold per pool > High Threshold
- **Clear Condition**: Actual percentage of IP addresses on hold per pool ≤ Low Threshold

Important: This command is overridden by the settings of the **alert-threshold** keyword of the **ip pool** command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are on high threshold percentage of *35* and a low threshold of *10* for an system using the Alarm thresholding model:

```
threshold ip-pool-hold 35 clear 10
```

threshold ip-pool-release

Sets an alert based on the percentage of IP addresses from an IP pool that are in the release state. This command affects all IP pools in the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold ip-pool-release *high_thresh* **[clear** *low_thresh* **]**

default threshold ip-pool-release

default

Configures the default setting.

threshold ip-pool-release *high_thresh*

Sets the high threshold percentage of addresses in the release state in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 100. Default: 0

clear *low_thresh*

Sets the low threshold percentage of addresses in the release state in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises below the low threshold within the polling interval, a clear alarm will be generated. It may be configured as an integer from 0 through 100. Default:0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

Use this command to set an alert or an alarm when the number of IP addresses the release state in any pool is equal to or greater than a specified percentage of the total number of addresses in the pool.
Alerts or alarms are triggered for percentage of IP address pool addresses in the release state based on the following rules:

- **Enter Condition**: Actual percentage of IP addresses in the release state per pool > High Threshold
- **Clear Condition**: Actual percentage of IP addresses in the release state per pool ≤ Low Threshold

Important: This command is overridden by the settings of the **alert-threshold** keyword of the **ip pool** command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are in the release state high threshold percentage of *35* and a low threshold of *10* for an system using the Alarm thresholding model:

```
threshold ip-pool-release 35 clear 10
```

threshold ip-pool-used

Sets an alert based on the percentage of IP addresses that have been assigned from an IP pool. This command affects all IP pools in the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold ip-pool-used *high_thresh* **[clear** *low_thresh* **]**

default threshold ip-pool-used

default

Configures the default setting.

threshold ip-pool-used *high_thresh*

Sets the high threshold percentage of addresses assigned from an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 100. Default: 0

clear *low_thresh*

Sets the low threshold percentage of addresses assigned from an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. It may be configured to any integer between 0 and 100. Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

Use this command to set an alert or an alarm when the number of IP addresses assigned from any pool is equal to or greater than a specified percentage of the total number of addresses in the pool.
Alerts or alarms are triggered for percentage of IP address pool addresses used based on the following rules:

- **Enter Condition**: Actual percentage of IP addresses used per pool > High Threshold
- **Clear Condition**: Actual percentage of IP addresses used per pool ≤ Low Threshold

Important: This command is overridden by the settings of the **alert-threshold** keyword of the **ip pool** command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are used high threshold percentage of *35* and a low threshold of *10* for an system using the Alarm thresholding model:

```
threshold ip-pool-used 35 clear 10
```

threshold monitoring

Enables or disables thresholds alerting for a group of thresholds.

Product

All

Privilege

Security Administrator, Administrator

Syntax

`[ default | no ] threshold monitoring available-ip-pool-group`

`default`

Configures the default setting.

`no`

Disables threshold monitoring for the specified value.

`threshold monitoring available-ip-pool-group`

Enables threshold monitoring for IP pool thresholds at the context level and the IP address pool-level. Refer to the **`threshold available-ip-pool-group`** command, the **`threshold ip-pool-x`** commands and the **`alert-threshold`** keyword of the **`ip pool`** command for additional information on these values.

Usage

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the *SNMP MIB Reference*.

The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.
- **Alarm System:** High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists and/or a condition clear alarm is generated.

"Outstanding" alarms are reported to through the system's alarm subsystem and are viewable through the CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

Table 17. Thresholding Reporting Mechanisms by Model

Model	SNMP Traps	Logs	Alarm System
Alert	X	X	
Alarm	X	X	X

Refer to the **`threshold poll`** command in Global Configuration Mode Commands for information on configuring the polling interval over which IP address pool utilization is monitored.

Example

the following command enables threshold monitoring for IP pool thresholds at the context level and the IP address pool-level:

```
threshold monitoring available-ip-pool-group
```

threshold pdsn-service init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for a PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

threshold pdsn-service init-rrq-rcvd-rate *high_thresh* **[clear** *low_thresh* **]**

no threshold pdsn-service init-rrq-rcvd-rate

no

Deletes the alert or alarm.

threshold pdsn-service init-rrq-rcvd-rate *high_thresh*

Sets the high threshold average number of calls setup per second that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer between 0 and 1000000. Default: 0

clear *low_thresh*

Sets the low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured as an integer between 0 and 1000000. Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the average number of calls setup per second is equal to or less than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter Condition**: Actual number of calls setup per second > High Threshold
- **Clear Condition**: Actual number of calls setup per second ≤ Low Threshold

Example

The following command configures a number of calls setup per second threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold pdsn-service init-rrq-rcvd-rate 1000 clear 500
```

udr-module active-charging-service

Enables creation, configuration and deletion of the User Data Record (UDR) module for the context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] udr-module active-charging-service
```

no

Deletes the UDR module configuration for the current context.

udr-module active-charging-service

Enables the UDR module configuration for the current context.

Usage

Use this command to create the UDR module for the context, and configure the UDR module for active charging service records. You must be in a non-local context when specifying this command, and you must use the same context when specifying the EDR module command.

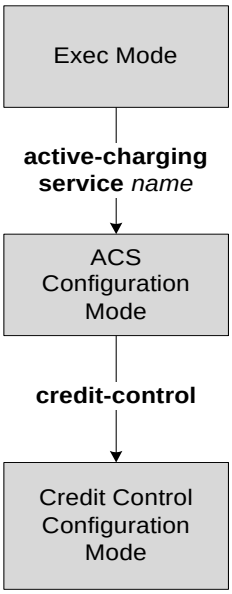
Example

The following command creates the UDR module for the context, and enters the UDR Module Configuration Mode:

```
udr-module active-charging-service
```

Chapter 54
Credit Control Configuration Mode Commands

The Credit Control Configuration Mode is used to configure prepaid services for Diameter/RADIUS applications.



apn-name-to-be-included

This command configures whether the virtual or real Access Point Name (APN) is sent in Credit Control Application (CCA) messaging.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
apn-name-to-be-included { gn | virtual }

default apn-name-to-be-included
```

default

Configures this command with the default setting.
Default: **gn**

gn

Sends the Gn APN name in the CCA messages.

virtual

Sends the virtual APN name, if configured in the APN Configuration Mode, in the CCA messages.

Usage

Use this command to configure the APN information in CCA messages. Virtual APN name can be set to be sent in CCA messages if it is configured in the APN Configuration Mode.

Example

The following command sets the virtual APN name to be sent in CCA message:

```
apn-name-to-be-included virtual
```

app-level-retransmission

This command enables/disables application-level retransmissions with the “T” bit set.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
app-level-retransmission { set-retransmission-bit | unset-retransmission-bit }

default app-level-retransmission
```

default

Configures this command with the default setting.
Default: **unset-retransmission-bit**

set-retransmission-bit

Sets the retransmission bit.

unset-retransmission-bit

Unsets the retransmission bit.

Usage

Use this command to enable application-level transmission with “T” bit set.
'T' bit setting is done only for DIABASE protocol-based rerouting and not for application-based retransmissions. In order to identify such retransmissions, the server expects the T bit to be set at all levels (both DIABASE and application) of retransmission, which can be achieved with this CLI command.

Example

The following command specifies to set retransmission bit:

```
app-level-retransmission set-retransmission-bit
```

diameter dictionary

This command configures the Diameter Credit Control dictionary for the Active Charging Service (ACS).

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
diameter dictionary { dcca-custom1 | dcca-custom10 | dcca-custom11 | dcca-custom12 |
dcca-custom13 | dcca-custom14 | dcca-custom15 | dcca-custom16 | dcca-custom17 | dcca-
custom18 | dcca-custom19 | dcca-custom2 | dcca-custom20 | dcca-custom21 | dcca-custom22 |
dcca-custom23 | dcca-custom24 | dcca-custom25 | dcca-custom26 | dcca-custom27 | dcca-
custom28 | dcca-custom29 | dcca-custom3 |  dcca-custom30 | dcca-custom4 | dcca-custom5 |
dcca-custom6 | dcca-custom7 | dcca-custom8 | dcca-custom9 | standard }

default diameter dictionary
```

default

Configures this command with the default setting.
Default: standard dictionary

dcca-custom1 ... dcca-custom30

Specifies a custom Diameter dictionary.

standard

Specifies the standard Diameter dictionary.
Default: Enabled

Usage

Use this command to select the Diameter dictionary for ACS.

Example

The following command selects the standard Diameter dictionary:

```
diameter dictionary standard
```

diameter dynamic-rules request-quota

This command specifies to request quota immediately in the CCR sent to the Gy interface when the traffic matches the dynamic rules with Online AVP enabled and received over Gx interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
diameter dynamic-rules request-quota { on-traffic-match | on-receiving-rule }

default diameter dynamic-rules request-quota
```

default

Configures this command with the default setting.
Default: **on-receiving-rule**

on-traffic-match

Requests quota only when there is traffic matching the dynamic rules with Online AVP enabled.

on-receiving-rule

Requests quota on receiving a dynamic rule with Online AVP enabled.

Usage

Use this command to request quota when the traffic matches the dynamic rules with Online AVP enabled.

Example

The following command specifies to request quota on receiving a dynamic rule with Online AVP enabled:

```
diameter dynamic-rules request-quota on-receiving-rule
```

diameter fui-redirected-flow

This command enables to control the behavior of marking redirected HTTP flow as free-of-charge.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] diameter fui-redirected-flow allow
```

no

Disables the behavior of marking redirected HTTP flow as free-of-charge.
Default: **diameter fui-redirected-flow allow**

Usage

Use this command to control the behavior of marking redirected HTTP flow as free-of-charge when the Final-Unit-Indication (FUI) Diameter AVP comes without Filter IDs.

Important: Note that the default value, when configured, does not appear in the output of the **show configuration** command output; instead appear only in the output of the **show configuration verbose** command. When the HTTP redirection feature is disabled using the **no diameter fui-redirected-flow allow** command, it will be appear in the output of the **show configuration** command.

Example

The following command specifies to allow the packets free of charge, when matching the redirected-flow:

```
diameter fui-redirected-flow allow
```

diameter gsu-with-only-infinite-quota

This command configures whether to accept/reject CCA messages that contain Granted-Service-Unit AVP with only infinite quota grants from the server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
diameter gsu-with-only-infinite-quota { accept-credit-control-answer | reject-credit-control-answer }

default diameter gsu-with-only-infinite-quota
```

default

Configures this command with the default setting.
Default: **reject-credit-control-answer**

accept-credit-control-answer

Accepts the Credit-Control-Answer message.

reject-credit-control-answer

Rejects the Credit-Control-Answer message.

Usage

Use this command to accept/reject CCA messages that contain the Granted-Service-Unit AVP with only infinite quota grants from the server.

Example

The following command specifies to accept CCA with the Granted-Service-Unit AVP containing only Infinite quota:

```
diameter gsu-with-only-infinite-quota accept-credit-control-answer
```

diameter ignore-returned-rulebase-id

This command configures to accept/ignore the rulebase ID in the Rulebase-Id AVP returned by the Diameter server in CCA messages.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] diameter ignore-returned-rulebase-id
```

default

Configures this command with the default setting.
Default: Accept

no

Accepts the rulebase ID received from Diameter server in CCA.

Usage

Use this command to ignore/accept rulebase ID returned from the Diameter server in CCA.

Example

The following command ignores the rulebase ID returned from the Diameter server in CCA:

```
diameter ignore-returned-rulebase-id
```

diameter ignore-service-id

This command enables to accept/ignore service ID in the Service-Identifier AVP defined in the Diameter dictionaries. This command is applicable to all products that use the Gy interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] diameter ignore-service-id
```

default

Configures this command with the default setting.
Default: Accept

no

Specifies to accepts the service ID.

Usage

Use this command to ignore/accept service ID value in the Service-Identifier AVP in the Diameter dictionaries for Gy interface implementations.
This command can be used to disable the usage of the Service-Identifier AVP for Gy interface implementations even if any of the Diameter dictionaries support the Service-Identifier AVP, and if this AVP should not be used for Gy interactions but must be present in GCDRs/eGCDRs.

Example

The following command specifies to ignore service ID in the Diameter dictionaries:

```
diameter ignore-service-id
```

diameter mscc-final-unit-action terminate

This command enables either to terminate a PDP session immediately when the Final-Unit-Action (FUA) in a particular Multiple Service Credit Control (MSCC) is set as TERMINATE and the quota is exhausted for that service, or to terminate the session after all other MSCCs (categories) have used up their available quota.

Important: This command is available only in 10.2 and later releases.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
diameter mscc-final-unit-action terminate { category | session { on-per-mscc-exhaustion |
on-all-mscc-exhaustion } }

default diameter mscc-final-unit-action terminate
```

default

Configures this command with the default setting.
Default: Same as **diameter mscc-final-unit-action terminate category**

category

This is the standard behavior wherein the category is terminated if the Final-Unit-Indication AVP comes with TERMINATE for a given MSCC.

session { on-per-mscc-exhaustion | on-all-mscc-exhaustion }

Terminates the session depending on the quota usage of one MSCC or all the MSCCs.
on-per-mscc-exhaustion: When the FUA in a particular MSCC is set as TERMINATE and the quota is exhausted for that service, the session will be terminated immediately regardless of the state of the other MSCCs.
on-all-mscc-exhaustion: When the FUA in a particular MSCC is set as TERMINATE and the quota is exhausted for that service, the session termination will be initiated after all the other MSCCs (categories) have used up their available quota. There will no more CCR(U) messages sent requesting quota after receiving the FUA as TERMINATE in the MSCC level.

Usage

Use this command to terminate a PDP session immediately when the FUA in a particular MSCC is set as TERMINATE and the quota is exhausted for that service, or to terminate the session after all other MSCCs (categories) have used up their available quota.

Example

The following command terminates the PDP session after quota exhausts for all MSCCs when MSCC FUA is set to TERMINATE:

```
diameter mscc-final-unit-action terminate session on-all-mscc-exhaustion
```

diameter mscc-per-ccr-update

This command configures sending single/multiple Multiple-Services-Credit-Control (MSCC) AVP in CCR-U messages.

Important: This command is available only in 8.3 and later releases.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
diameter mscc-per-ccr-update { multiple | single }

default diameter mscc-per-ccr-update
```

default

Configures this command with the default setting.
Default: **multiple**

multiple

Sends multiple Multiple-Services-Credit-Control AVP in a single CCR-U message.

single

Sends only one Multiple-Services-Credit-Control AVP in a CCR-U message.

Usage

Use this command to configure sending single/multiple Multiple-Services-Credit-Control AVP in CCR-U messages.

Example

The following command configures sending a single Multiple-Services-Credit-Control AVP in CCR-U messages:

```
diameter mscc-per-ccr-update single
```

diameter origin host

This command is obsolete. See the diameter origin endpoint command.

diameter origin endpoint

This command configures the Diameter Credit Control Origin Endpoint.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter origin endpoint *endpoint_name* **[realm** *realm_name* **]**

no diameter origin endpoint

no

Removes the Diameter Credit Control Origin Endpoint configuration.

endpoint *endpoint_name*

Specifies the Diameter Credit Control Origin Endpoint name as an alphanumeric string of 1 through 63 characters.

realm *realm_name*

Specifies the Diameter Credit Control Realm ID as an alphanumeric string of 1 through 127 characters.

Usage

Use this command to configure the Diameter Credit Control Origin Endpoint.
The endpoint to configure should be pre-configured. For information on creating and configuring a Diameter endpoint, see the **diameter endpoint** command in the Context Configuration mode.

Example

The following command configures a Diameter Credit Control Origin Endpoint named *test*:

```
diameter origin endpoint test
```

diameter peer-select

This command configures the Diameter credit control primary and secondary hosts for DCCA.

Product

All

Privilege

Security Administrator, Administrator

Syntax

In 8.x and earlier releases:

diameter peer-select peer *peer_name* **[realm** *realm_name* **] [secondary-peer** *secondary_peer_name* **[realm** *realm_name* **]] [imsi-based start-value** *imsi_start_value* **end-value** *imsi_end_value* **]**

no diameter peer-select [imsi-based start-value *imsi_start_value* **end-value** *imsi_end_value* **]**

In 9.0 and later releases, for UMTS deployments:

diameter peer-select peer *peer_name* **[realm** *realm_name* **] [secondary-peer** *secondary_peer_name* **[realm** *realm_name* **]] [imsi-based { { prefix | suffix }** *imsi/prefix/suffix_start_value* **} [to** *imsi/prefix/suffix_end_value* **]] [msisdn-based { { prefix | suffix }** *msisdn-based/prefix/suffix_start_value* **} [to** *msisdn-based/prefix/suffix_end_value* **]]**

no diameter peer-select [imsi-based { { prefix | suffix } *imsi/prefix/suffix_start_value* **} [to** *imsi/prefix/suffix_end_value* **]] | [msisdn-based { { prefix | suffix }** *msisdn-based/prefix/suffix_start_value* **} [to** *msisdn-based/prefix/suffix_end_value* **]]**

no

Removes previously configured Diameter credit control peer selection setting.

peer *peer_name*

Specifies the primary host name. as an alphanumeric string of 1 through 63 characters that can contain punctuation characters.

imsi-based start-value *imsi_start_value* **end-value** *imsi_end_value*

Important: This section applies only to 8.3 and earlier releases.

Specifies peer selection based on International Mobile Subscriber Identification (IMSI) range. **start-value** *imsi_start_value* specifies the start of range in integer value of IMSI, and **end-value** *imsi_end_value* specifies the end of range in integer value of IMSI.

imsi-based { { prefix | suffix } *imsi/prefix/suffix_start_value* } [to *imsi/prefix/suffix_end_value*]

Important: This section applies only to 9.0 and later releases for UMTS deployments.

Selects peer based on IMSI prefix or suffix or IMSI range.
prefix: Specifies the prefix range
suffix: Specifies the suffix range
imsi/prefix/suffix_start_value: Specifies the IMSI/prefix/suffix start value. *prefix/suffix* must be an IMSI prefix/suffix, and must be an integer from 1 through 15 characters.
imsi/prefix/suffix_end_value: Specifies the IMSI/prefix/suffix end value. *prefix/suffix* must be an IMSI prefix/suffix, and must be an integer from 1 through 15 characters that must be greater than the start value.

Important: If prefix/suffix is used, the lengths of both start and end prefix/suffix must be equal. If the **prefix** or **suffix** keyword is not specified, it will be considered as suffix.

msisdn-based { { prefix | suffix } *msisdn/prefix/suffix_start_value* } [to *msisdn/prefix/suffix_end_value*]

Specifies peer selection based on MSISDN prefix or suffix or MSISDN range.
prefix: Specifies the prefix range
suffix: Specifies the suffix range
msisdn/prefix/suffix_start_value: Specifies the MSISDN/prefix/suffix start value. *prefix/suffix* must be an MSISDN prefix/suffix, and must be an integer from 1 through 15 characters.
msisdn/prefix/suffix_end_value: Specifies the MSISDN/prefix/suffix end value. *prefix/suffix* must be an MSISDN prefix/suffix, and must be an integer from 1 through 15 characters that must be greater than the start value.

realm *realm_name*

The *realm_name* must be an alphanumeric string of 1 through 127 characters, and can contain punctuation characters. The realm may typically be a company or service name.

secondary-peer *secondary_peer_name*

Specifies a name for the secondary host to be used for failover processing. When the route-table does not find an AVAILABLE route, the secondary host performs a failover processing if the diameter session failover command is set.
secondary_peer_name must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters.

Usage

Use this command to configure Diameter credit control host selection.
If the **diameter peer-select** command is not configured, and if multiple peers are configured in the endpoint, the available peers configured in the endpoint are automatically chosen in a load-balanced round-robin manner.
StarOS 9.0 and later releases support peer selection using prefix or suffix of IMSI or IMSI range. Subscribers are now assigned to a primary OCS instance based on the value of the IMSI prefix or suffix of a length of 1 to 15 digits. If the prefix or suffix keyword is not specified, it will be considered as suffix. Up to 64 peer selects

can be configured. At a time either prefix or suffix mode can be used in one DCCA config. If prefix or suffix mode is used, the lengths of all prefix/suffix must be equal.
In 12.2 and later releases, Diameter peer selection can also be performed based on the configurable prefix or suffix of MSISDN or MSISDN range.
Each primary OCS may have a designated secondary OCS in case of failure of the primary. It will be the responsibility of the GGSN to use the appropriate secondary OCS in case of primary failure. The secondary OCS for each primary OCS will be one of the existing set of OCSs.

Example

The following command configures a Diameter credit control peer named *test* and the realm *companyx*:

```
diameter peer-select peer test realm companyx
```

The following command configures IMSI-based Diameter credit control peer selection in the IMSI range of *1234567890* to *1234567899*:

```
diameter peer-select peer star imsi-based start-value 1234567890 end-
value 1234567899
```

The following command configures IMSI-based DCCA peer selection with IMSI suffix of *100* through *200*:

```
diameter peer-select peer test_peer realm test_realm secondary-peer
test_sec_realm realm test_realm2 imsi-based suffix 100 to 200
```

diameter pending-timeout

This command configures the maximum time period to wait for response from a Diameter peer.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter pending-timeout *duration*

default diameter pending-timeout

default

Disables DCCA resending message at pending-timeout.

duration

Specifies the timeout duration (in seconds). The value must be an integer from 1 through 300.

after-expiry-try-secondary-host

This keyword is deprecated. This can now be managed using the **retry-after-tx-expiry** and **go-offline-after-tx-expiry** keywords in the failure-handling command.

Usage

Use this command to set the maximum time for Diameter credit control to receive a response from its peer. DCCA refers to this as the Tx Timer. Typically, this should be configured to a value smaller than the response-timeout value of Diameter Endpoint Configuration Mode. That value is typically too large for DCCA's purposes.

If DCCA gets a “no available routes” error before pending-timeout expires, then DCCA tries to send to the secondary host (if one has been configured). If DCCA gets no response and pending-timeout expires, then DCCA either tries the secondary host or gives up. This can now be managed using the failure-handling command.

If routing has failed, i.e., the attempt to the primary host, as well as, the attempt to the secondary host (if that has been configured), then the processing configured by the failure-handling command is performed.

The routing (i.e., returning a good response, no response or an error response such as "no available routes") is controlled by Diameter Endpoint Configuration Mode. That uses a watchdog timer (called Tw Timer) to attempt a different route to a host. Multiple routes could be attempted. If there's no response before the endpoint's configured response-timeout expires, then "no available routes" is the routing result. The routing logic remembers the status of routes, so it can return "no available routes" immediately, without using any timers.

The default case will disable DCCA resending message at Tx (pending-timeout). So messages are retried only at Tw (device watchdog timeout) by diabase or at response-timeout by DCCA.

Example

The following command configures a Diameter Credit Control Pending Timeout setting of *20* seconds:

```
diameter pending-timeout 20
```

diameter result-code

This command enables sending a GTP Create-PDP-Context-Rsp message with cause code based on the DCCA result code.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter result-code { authorization-rejected | credit-limit-reached | end-user-service-denied | user-unknown } use-gtp-cause-code { authentication-failure | no-resource-available | system-failure }

default diameter result-code { authorization-rejected | credit-limit-reached | end-user-service-denied | user-unknown } use-gtp-cause-code

default

Configures this command with the default setting.
In 12.1 and earlier releases: **no-resource-available**
In 12.2 and later releases: **system-failure**

authorization-rejected

Result code received as DIAMETER_AUTHORIZATION_REJECTED(5003).

credit-limit-reached

Result code received as DIAMETER_CREDIT_LIMIT_REACHED(4012).

end-user-service-denied

Result code received as DIAMETER_END_USER_DENIED(4010).

user-unknown

Result code received as DIAMETER_USER_UNKNOWN(5030).

use-gtp-cause-code

Cause code to be sent in GTP response.

authentication-failure

Sends the GTP cause code GTP_USER_AUTHENTICATION_FAILED in GTP response.

no-resource-available

Sends the GTP cause code GTP_NO_RESOURCES_AVAILABLE in GTP response.

system-failure

Sends the GTP cause code GTP_SYSTEM_FAILURE in GTP response.

Usage

On receiving result-code as AUTHORIZATION-REJECTED, CREDIT_LIMIT_REACHED, END_USER_DENIED or USER_UNKNOWN from DCCA server, based on this CLI configuration, in GTP Create-PDP-Context Response message the cause code can either be sent as GTP_NO_RESOURCE_AVAILABLE or GTP_AUTHENTICATION_FAILED or GTP_SYSTEM_FAILURE.

Example

The following command sets the deny cause as user authentication failure when the CCA-Initial has the result code DIAMETER_AUTHORIZATION_REJECTED(5003):

```
diameter result-code authorization-rejected use-gtp-cause-code
authentication-failure
```

diameter send-ccri

This command configures when to send an initial Credit Control Request (CCR-I) for the subscriber session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
diameter send-ccri { session-start | traffic-start }

default diameter send-ccri
```

default

Configures this command with the default setting.
Default: **session-start**

session-start

Sends CCR-I when the PDP context is being established (on receiving Create-PDP-Context-Request).

traffic-start

Delays sending CCR-I until the first data packet received from the subscriber.

Usage

Use this command to configure when to send CCR-Initial for the subscriber session.

Example

The following command configures to send CCR-I on traffic detection and not on context creation:

```
diameter send-ccri traffic-start
```

diameter service-context-id

This command configures the value to be sent in the Service-Context-Id AVP, which identifies the context in which DCCA is used.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter service-context-id *service_context_id*

default diameter service-context-id

default

Configures this command with the default setting. Currently, the default value is encoded based on the dictionary wherever applicable; when not applicable, it is not encoded.

service_context_id

Specifies the service context as an alphanumeric string of 1 through 63 characters that can contain punctuation characters.

Usage

If Service-Context-Id is applicable and configured using this command, it will be sent in the AVP Service-Context-Id in the Diameter CCR message.

Example

The following command specifies the value *version@customer.com* to be sent in the Service-Context-Id AVP in the Diameter CCR message:

```
diameter service-context-id version@customer.com
```

diameter session failover

This command enables/disables Diameter Credit Control Session Failover. When enabled, the secondary peer is used in the event the main peer is unreachable.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] diameter session failover
```

default

Configures this command with the default setting.
Default: Depends on the **failure-handling** configuration

no

If the primary server is not reachable, failover is not triggered and the session is torn down. No failover action is taken.

Usage

Use this command to enable/disable Diameter Credit Control Session Failover.
The failure-handling configuration comes into effect only if **diameter session failover** is present in the configuration. The failover can be overridden by the server in the response message, and it takes precedence.

Example

The following command enables Diameter Credit Control Session Failover:

```
diameter session failover
```

diameter update-dictionary-avps

This command enables dictionary control of the AVPs that need to be added based on the version of the specification with which the Online Charging System (OCS) is compliant. This command is applicable to all products that use the dcca-custom8 dictionary for Gy interface implementation.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
diameter update-dictionary-avps { 3gpp-rel8 | 3gpp-rel9 }

[ default | no ] diameter update-dictionary-avps
```

default | no

Configures this command with the default setting.
Default: Compliant with the oldest release (Rel. 7) and send only Rel. 7 AVPs

3gpp-rel8

Select the 3GPP Rel. 8 AVPs for encoding.

3gpp-rel9

Selects the 3GPP Rel. 9 AVPs for encoding.

Usage

Important: This command is applicable ONLY to the dcca-custom8 dictionary. If, for any dictionary other than dcca-custom8, this command is configured with a value other than the default, configuration errors will be indicated in the output of the **show configuration errors section active-charging** command.

Use this command to encode the AVPs in the dictionary based on the release version of the specification to which the OCS is compliant with.

Example

The following command enables encoding of AVPs in the dictionary based on 3GPP Rel. 9:

```
diameter update-dictionary-avps 3gpp-rel9
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

failure-handling

This command configures Diameter Credit Control Failure Handling (CCFH) behavior in the event of communication failure with the prepaid server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
failure-handling { initial-request | terminate-request | update-request } { continue [
go-offline-after-tx-expiry | retry-after-tx-expiry ] | retry-and-terminate [ retry-after-
tx-expiry ] | terminate }

default failure-handling [ initial-request | terminate-request | update-request ]
```

---

default failure-handling [initial-request | terminate-request | update-request]

Configures the default CCFH setting.
initial-request: The default setting is **terminate**.
update-request: The default setting is **retry-and-terminate**.
terminate-request: The default setting is **retry-and-terminate**.

---

initial-request

Specifies the message type as CCR-Initial.

---

terminate-request

Specifies the message type as CCR-Terminate.

---

update-request

Specifies the message type as CCR-Update.

---

continue

Specifies the CCFH setting as continue. The online session is converted into an offline session. The associated PDP Context is established (new sessions) or not released (ongoing sessions).

---

retry-and-terminate

Specifies the CCFH setting as retry-and-terminate. The user session will continue for the duration of one retry attempt with the prepaid server. If there is no response from both primary and secondary servers, the session is torn down.

---

terminate

Specifies the CCFH setting as terminate. All type of sessions (initial or update) are terminated in case of failure.

go-offline-after-tx-expiry

Starts offline charging after Tx expiry.

retry-after-tx-expiry

Retries after Tx expiry. Enables secondary-host, if up, to take over after Tx expiry.

Usage

Use this command to select the CCFH behavior. The specified behavior is used for sessions when no behavior is specified by the prepaid server. By default, the CCFH is taken care at response-timeout except for terminate setting.
If the Credit-Control-Failure-Handling AVP is received from the server, the received setting will be applied to all the message types.
The following table indicates the CCFH behavior for the combination of different CCFH settings, and the corresponding CLI commands.

CCFH Setting	CLI Command	Behavior at Tx	Behavior at RT	Secondary is Up	Secondary is Down
Initial-request Message Type					
Continue	**initial-request continue**	N/A	Continue	Secondary takes over after RT	Offline after another RT. No more quota requests are performed for any rating group within the session after DCCA failure (even if connectivity to DCCA is restored)
	initial-request continue go-offline-after-tx-expiry	Offline	N/A	Offline at Tx	Offline at Tx
	initial-request continue retry-after-tx-expiry	Continue	N/A	Secondary takes over after Tx	Offline after another Tx
Retry-and-terminate	**initial-request retry-and-terminate**	N/A	Retry	Secondary takes over after RT	Terminate after another RT
	initial-request retry-and-terminate retry-after-tx-expiry	Retry	N/A	Secondary takes over after Tx	Terminate after another Tx
Terminate	**initial-request terminate**	Terminate	N/A	Terminate after Tx	Terminate after Tx
Update-request Message Type					
Continue	**update-request continue**	N/A	Continue	Secondary takes over after RT	Offline after another RT
	update-request continue go-offline-after-tx-expiry	Offline	N/A	Offline at Tx	Offline at Tx

CCFH Setting	CLI Command	Behavior at Tx	Behavior at RT	Secondary is Up	Secondary is Down
	update-request continue retry-after-tx-expiry	Continue	N/A	Secondary takes over after Tx	Offline after another Tx
Retry-and-terminate	**update-request retry-and-terminate**	N/A	Retry	Secondary takes over after RT	Sends CCR-T after another RT
	update-request retry-and-terminate retry-after-tx-expiry	Retry	N/A	Secondary takes over after Tx	Sends CCR-T after another Tx
Terminate	**update-request terminate**	Terminate	N/A	Sends CCR-T after Tx	Sends CCR-T after Tx
Terminate-request Message Type					
Continue	**terminate-request continue**	N/A	Retry	CCR-T is sent to secondary after RT	Terminate after another RT
	terminate-request continue go-offline-after-tx-expiry	Retry	N/A	CCR-T is sent to secondary after Tx	Terminate after another Tx
	terminate-request continue retry-after-tx-expiry	Retry	N/A	CCR-T is sent to secondary after Tx	Terminate after another Tx
Retry-and-terminate	**terminate-request retry-and-terminate**	N/A	Retry	CCR-T is sent to secondary after RT	Terminate after another RT
	terminate-request retry-and-terminate retry-after-tx-expiry	Retry	N/A	CCR-T is sent to secondary after Tx	Terminate after another Tx
Terminate	**terminate-request terminate**	Terminate	N/A	Terminate after Tx	Terminate after Tx

Example

The following command sets the Credit Control Failure Handling behavior for initial request message type to **retry-and-terminate**:

```
failure-handling initial-request retry-and-terminate
```

mode

This command configures the Prepaid Credit Control mode to RADIUS or Diameter.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
mode { diameter | radius }

default mode
```

default

Configures the default prepaid credit control mode.
Default: **diameter**

diameter

Enables Diameter Credit Control Application (DCCA) for prepaid charging.

radius

Enables RADIUS Credit Control for prepaid charging.

Usage

Use this command to configure the prepaid charging application mode to Diameter or RADIUS credit control.

Example

The following command specifies to use RADIUS prepaid credit control application:

```
mode radius
```

pending-traffic-treatment

This command controls the pass/drop treatment of traffic while waiting for definitive credit information from the server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
pending-traffic-treatment { { { forced-reauth | trigger | validity-expired } drop | pass
} | { { noquota | quota-exhausted } buffer | drop | limited-pass volume | pass } }

default pending-traffic-treatment { forced-reauth | noquota | quota-exhausted | trigger |
validity-expired }
```

default

Configures this command with the default setting.
Default: **drop**

forced-reauth

Sets the Diameter credit control pending traffic treatment to forced reauthorization.

trigger

Sets the Diameter credit control pending traffic treatment to trigger.

validity-expired

Sets the Diameter credit control pending traffic treatment to validity expired.

noquota

Sets the Diameter credit control pending traffic treatment to no quota.

quota-exhausted

Sets the Diameter credit control pending traffic treatment to quota exhausted.

buffer

Specifies to tentatively count/time traffic, and then buffer traffic pending arrival of quota. Buffered traffic will be forwarded and fully charged against the quota when the quota is eventually obtained and the traffic is passed.

drop

Drops any traffic when there is no quota present.

limited-pass *volume*

Enables limited access for subscribers when the OCS is unreachable.
volume specifies the Default Quota size (in bytes) and must be an integer from 1 through 4294967295.

This feature allows the subscriber to use the network when the OCS response is slow. This configuration enables to set a Default Quota size from which the subscriber can consume quota until response from the OCS arrives. The traffic consumed by the subscriber from the Default Quota at the beginning of the session is reported and counted against the quota assigned from the OCS.
Default Quota is not used for subsequent credit requests.
If the Default Quota is NOT exhausted before the OCS responds with quota, traffic is allowed to pass. Initial Default Quota usage is counted against initial quota allocated. If quota allocated is less than the actual usage, the actual usage and request additional quota are reported. If no additional quota is available, the traffic is denied.
If the Default Quota is NOT exhausted before the OCS responds with denial of quota, traffic is blocked after the OCS response. The gateway will report usage on Default Quota even in for CCR-U (FINAL) or CCR-T until the OCS responds.
If the Default Quota is exhausted before the OCS responds, the session is dropped.
The default pending-traffic-treatment for **noquota** is drop. The **default pending-traffic-treatment noquota** command removes any Default Quota limit configured.

pass

Passes all traffic more or less regardless of quota state.

Usage

Use this command to set the Diameter credit control pending traffic treatment while waiting for definitive credit information from the server.
This CLI command is different than the **failure-handling** command, which specifies behavior in the case of an actual timeout or error, as opposed to the behavior while waiting. See also the **buffering-limit** command in the Active Charging Service Configuration Mode.

Example

The following command sets the Diameter credit control pending traffic treatment to drop any traffic when there is no quota present:

```
pending-traffic-treatment noquota drop
```

quota

This command sets various time-based quotas in the prepaid credit control service.

Product

All

Privilege

Security Administrator, Administrator

Syntax

quota *holding_time* **| validity-time** *validity_time* **}**

{ default | no } quota { holding-time | validity-time }

holding-time *holding_time*

Specifies the Quota Holding Time (QHT) in seconds. The value must be an integer from 1 through 4000000000.

validity-time *validity_time*

Specifies the validity lifetime of the quota, in seconds. The value must be an integer from 1 through 65535.

Usage

Use this command to set the prepaid credit control quotas.

Example

The following command sets the prepaid credit control request holding time to *30000* seconds:

```
quota holding-time 30000
```

quota request-trigger

This command configures the action on the packet that triggers the credit control application to request quota.

Product

All

Privilege

Security Administrator, Administrator

Syntax

quota request-trigger { exclude-packet-causing-trigger | include-packet-causing-trigger }

{ default | no } quota request-trigger

default quota request-trigger

Configures this command with the default setting. Default: **include-packet-causing-trigger**

no

Same as the **default quota request-trigger** command.

Important: In 10.0 and later releases, this keyword is deprecated.

exclude-packet-causing-trigger

Excludes the packet causing threshold limit violation trigger.

include-packet-causing-trigger

Includes the packet causing the threshold limit violation trigger.

Usage

Use this command to configure action on the packet that triggers the credit control application to request quota, whether the packet should be excluded/included in the utilization information within the quota request.

Example

The following command sets the system to exclude the packets causing threshold limit triggers from accounting of prepaid credit of a subscriber:

```
quota request-trigger exclude-packet-causing-trigger
```

quota time-threshold

This command configures the time threshold limit for subscriber quota in the prepaid credit control service.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
quota time-threshold { abs_time_value | percent percent_value }

{ default | no } quota time-threshold
```

default

Configures this command with the default setting.
Default: Disabled

no

Disables time threshold for prepaid credit control quota.

abs_time_value

Specifies the absolute threshold time (in seconds) for configured time quota in prepaid credit control charging. *abs_time_value* must be an integer from 1 through 86400. To disable this assign 0. Default: 0 (Disabled)

percent_value

Specifies the time threshold value as a percentage of the configured time quota in DCCA. *percent_value* must be an integer from 1 through 100.

Usage

Use this command to set the time threshold for prepaid credit control quotas.

Example

The following command sets the prepaid credit control time threshold to *400* seconds:

```
quota time-threshold 400
```

quota units-threshold

This command sets the unit threshold limit for subscriber quota in the prepaid credit control service.

Product

All

Privilege

Security Administrator, Administrator

Syntax

quota unit-threshold { *abs_unit_value* **| percent** *percent_value* **}**

{ default | no } quota units-threshold

default

Configures this command with the default setting.
Default: Disabled

no

Disables unit threshold for DCCA quota.

abs_unit_value

Specifies the absolute threshold value (in units) for the configured units quota in prepaid credit control application. *abs_unit_value* must be an integer from 1 through 4000000000. To disable this assign 0.
Default: 0 (Disabled)

percent_value

Specifies the time threshold value as a percentage of the configured units quota in DCCA. *percent_value* must be an integer from 1 through 100.

Usage

Use this command to set the units threshold for prepaid credit control quotas.

Example

The following command sets the prepaid credit control time threshold to *160400* units:

```
quota units-threshold 160400
```

quota volume-threshold

This command sets the volume threshold limit for subscriber quota in the prepaid credit control service.

Product

All

Privilege

Security Administrator, Administrator

Syntax

quota volume-threshold { *abs_vol_value* | percent *percent_value* }

{ default | no } quota volume-threshold

default

Configures this command with the default setting.
Default: Disabled

no

Disables volume threshold for prepaid credit control quota.

abs_vol_value

Specifies the absolute threshold volume (in bytes) to the configured volume quota in prepaid credit control. *abs_vol_value* must be an integer from 1 through 4000000000. To disable this assign 0. Default: 0 (Disabled)

percent *percent_value*

Specifies the volume threshold value as a percentage of the configured volume quota in prepaid credit control. *percent_value* must be an integer from 1 through 100.

Usage

Use this command to set the volume threshold for prepaid credit control quotas.

Example

The following command sets the prepaid credit control volume threshold to *160400* bytes:

```
quota volume-threshold 160400
```

radius usage-reporting-algorithm

This command configures the usage reporting algorithm for RADIUS prepaid using the Diameter Credit-Control Application (DCCA).

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
radius usage-reporting-algorithm { cumulative | relative }

default radius usage-reporting-algorithm
```

default

Configures this command with the default setting.
Default: **cumulative**

cumulative

Reports the total accumulated usage of quota in every accounting interim.

relative

Reports the quota usage per accounting interim (since the previous usage report).

Usage

Use this command to configure the usage reporting algorithm for RADIUS prepaid using DCCA.

Example

The following command configures the usage reporting algorithm for RADIUS prepaid using DCCA to *relative*:

```
radius usage-reporting-algorithm relative
```

redirect-indicator-received

This command configures the action on buffered packets when a redirect-indicator is received from the RADIUS server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect-indicator-received { discard-buffered-packet | reprocess-buffered-packet }

{ default | no } redirect-indicator-received
```

default

Configures this command with the default setting. Default: **discard-buffered-packet**

no

Disables the redirect-indicator-received configuration.

discard-buffered-packet

Discards the buffered packet.

reprocess-buffered-packet

Redirects the buffered packet on receiving a redirect-indicator from the RADIUS server.

Usage

Use this command to configure the action taken on buffered packet when redirect-indicator is received. Diameter can return a redirect URL but not a redirect indicator, however RADIUS can return a redirect indicator. In this situation, any subsequent subscriber traffic would match ruledefs configured with cca redirect-indicator, and charging actions that have flow action redirect-url should be configured. However, some handsets do not retransmit, so there will be no subsequent packets. On configuring reprocess-buffered-packet, the ruledefs are reexamined to find a new charging action, which may have flow action redirect-url configured.

Example

The following command configures the action taken on buffered packet when redirect-indicator is received to reprocess-buffered-packet:

```
redirect-indicator-received reprocess-buffered-packet
```

servers-unreachable

This command configures whether to continue or terminate calls when Diameter server(s) or the OCS become unreachable.

Product

All

Privilege

Security Administrator, Administrator

Syntax

In 12.1 and earlier releases:

```
servers-unreachable { initial-request { continue | terminate [ after-timer-expiry timeout_period ] } | update-request { continue | terminate [ after-quota-expiry | after-timer-expiry timeout_period ] } }

no servers-unreachable { initial-request | update-request }
```

In 12.2 and later releases:

```
servers-unreachable { behavior-triggers { initial-request | update-request } transport-failure [ response-timeout | tx-expiry ] | initial-request { continue [ { [ after-interim-timetimeout_period ] [ after-interim-volume quota_value ] } server-retries retry_count ] | terminate [ { [ after-interim-time timeout_period ] [ after-interim-volume quota_value ] } server-retries retry_count | after-timer-expiry timeout_period ] } | update-request { continue [ { [ after-interim-time timeout_period ] [ after-interim-volume quota_value ] } server-retries retry_count ] | terminate [ { [ after-interim-time timeout_period ] [ after-interim-volume quota_value ] } server-retries retry_count ] | after-quota-expiry | after-timer-expiry timeout_period ] } }

no servers-unreachable { initial-request | update-request }

default servers-unreachable behavior-triggers { initial-request | update-request }
```

no

Deletes the current servers-unreachable configuration.

behavior-triggers { initial-request | update-request } transport-failure [response-timeout | tx-expiry]

This keyword is used to determine when to apply server-unreachable action. This supports three configurable options to apply server-unreachable action either at transport failure, Tx expiry or at response timeout. Out of these three options, the transport failure is the default option.

- **initial-request**: Specifies the behavior when Diameter server(s)/OCS become unreachable during initial session establishment.
- **update-request**: Specifies the behavior when Diameter server(s)/OCS become unreachable during mid-session.
- **transport-failure [response-timeout | tx-expiry]**: Specifies to trigger the behavior either at transport failure, response timeout or at Tx expiry.

initial-request { continue | terminate [after-timer-expiry *timeout_period* **] }**

Important: This section applies only to 12.1 and earlier releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during initial session establishment.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate [after-timer-expiry** *timeout_period* **]**: Specifies to terminate call if Diameter server(s) becomes unreachable.

  after-timer-expiry *timeout_period*: Specifies to terminate call after timeout period expires.

  timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.

initial-request { continue [{ [after-interim-time *timeout_period* **] [after-interim-volume** *quota_value* **] } server-retries** *retry_count* **] | terminate [{ [after-interim-time** *timeout_period* **] [after-interim-volume** *quota_value* **] } server-retries** *retry_count* **] | after-timer-expiry** *timeout_period* **}**

Important: This section applies only to 12.2 and later releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during initial session establishment.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate**: Specifies to terminate call if Diameter server(s) becomes unreachable.
  - **after-interim-time** *timeout_period*: Specifies to continue or terminate call after the interim timeout period expires.

    timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.
  - **after-interim-volume** *quota_value*: Specifies to continue or terminate call on exhaustion of the assigned quota.

    quota_value specifies the volume-based quota value, in bytes, and must be an integer from 1 through 4294967295.

    The **after-interim-volume** and **after-interim-time** can be configured in one of the following ways:
    - **after-interim-volume** *quota_value* **server-retries** *retry_count*
    - **after-interim-time** *timeout_period* **server-retries** *retry_count*
    - **after-interim-volume** *quota_value* **after-interim-time** *timeout_period* **server-retries** *retry_count*
  - **after-timer-expiry** *timeout_period*: Specifies to terminate call after timeout period expires.

    timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.
  - **server-retries** *retry_count*: Specifies the number of retries that should happen to OCS before allowing the session to terminate/offline.

retry_count specifies the retries to OCS, and must be an integer from 0 through 65535. If the value 0 is defined for this keyword, the retry to OCS will not happen instead the configured action will be immediately applied.

update-request { continue | terminate [after-quota-expiry | after-timer-expiry *timeout_period* **] }**

Important: This section applies only to 12.1 and earlier releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during mid session.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate [after-quota-expiry | after-timer-expiry** *timeout_period* **]**: Specifies to terminate call if Diameter server(s) becomes unreachable.
  - **after-quota-expiry**: Specifies to terminate call on exhaustion of all available quota.
  - **after-timer-expiry** *timeout_period*: Specifies to terminate call after timeout period expires.

    timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.

update-request { continue [{ [after-interim-time *timeout_period* **] [after-interim-volume** *quota_value* **] } server-retries** *retry_count* **] | terminate [{ [after-interim-time** *timeout_period* **] [after-interim-volume** *quota_value* **] } server-retries** *retry_count* **] | after-quota-expiry | after-timer-expiry** *timeout_period* **] }**

Important: This section applies only to 12.2 and later releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during mid session.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate**: Specifies to terminate call if Diameter server(s) becomes unreachable.
  - **after-interim-time** *timeout_period*: Specifies to continue or terminate call after the interim timeout period expires.

    timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.
  - **after-interim-volume** *quota_value*: Specifies to continue or terminate call on exhaustion of the assigned quota.

    quota_value specifies the volume-based quota value, in bytes, and must be an integer from 1 through 4294967295.

    The **after-interim-volume** and **after-interim-time** can be configured in one of the following ways:

    - **after-interim-volume** *quota_value* **server-retries** *retry_count*
    - **after-interim-time** *timeout_period* **server-retries** *retry_count*
    - **after-interim-volume** *quota_value* **after-interim-time** *timeout_period* **server-retries** *retry_count*

- **after-quota-expiry**: Specifies to terminate call on exhaustion of all available quota.
- **after-timer-expiry** *timeout_period*: Specifies to terminate call after timeout period expires.

  timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.
- **server-retries** *retry_count*: Specifies the number of retries that should happen to OCS before allowing the session to terminate/offline.

  retry_count specifies the retries to OCS, and must be an integer from 0 through 65535. If the value 0 is defined for this keyword, the retry to OCS will not happen instead the configured action will be immediately applied.

Usage

Use this command to configure whether to continue/terminate calls when Diameter server(s)/OCS are unreachable. This command can be used to verify the functionality of the configurable action if the OCS becomes unreachable.
In 12.1 and earlier releases, the OCS is considered down/unreachable when all transport/TCP connections are down for that OCS.
In 12.2 and later releases, the OCS is declared unreachable when all transport connections are down OR message timeouts happen (for example, a Tx expiry or response timeout, for all available OCS servers) owing to slow response from the OCS (may be due to network congestion or other network related issues).
The following set of actions are performed if the servers become unreachable:

- During initial session establishment:
  - Block traffic: Terminate the session.
  - Continue call: Continue by making the session offline.
  - Pass traffic until timer expiration post which terminates the call: Session would be offline while the timer is running.
  - Pass traffic until interim time expiration post which continues or terminates the call: Session would be offline while the timer is running.
  - Pass traffic until interim volume expiration post which continues or terminates the call: Session would be offline while the timer is running.
- During mid session:
  - Block traffic: Terminate the session.
  - Continue call: Continue by making the session offline.
  - Run out of session quota post which terminates the call.
  - Pass traffic until timer expiration post which terminates the call: Session would be offline while the timer is running.
  - Pass traffic until interim time expiration post which continues or terminates the call: Session would be offline while the timer is running.
  - Pass traffic until interim volume expiration post which continues or terminates the call: Session would be offline while the timer is running.

This command works on the same lines as the **failure-handling** command, which is very generic for each of the xxx-request and applies for Credit-Control-Failure-Handling (CCFH) during:

1. Application-level (Tx) timeout: Here message is sent out but server does not respond for the configured “pending-timeout” so application does CCFH actions.

2. Diabase-level request timeout: Here message is sent out but server does not respond and Diabase detects timeout of the application message and application does CCFH actions.
3. TCP connection error: Here message is NOT sent out due to no TCP connection and application does CCFH actions.

This CLI command is specifically for TCP connection error. The administrator can configure both of the following commands:

failure-handling initial-request continue

servers-unreachable initial-request terminate after-timer-expiry *30*

For conditions 1 and 2 described above, the **failure-handling** command will be applied, whereas for condition 3 both **failure-handling** and/or **servers-unreachable** commands can be used. This way, the operator has the flexibility to configure CCFH independent of OCS-unreachable feature, that is have two different failure handlings for same request types (as illustrated in the example above.)

Important: Please note that the flexibility to configure CCFH independent of OCS-unreachable feature is applicable only to 12.1 and earlier releases. In 12.2 and later releases, if configured, the **servers-unreachable** takes precedence over the **failure-handling** command.

If server returns the CC-Failure-Handling AVP, it would apply for conditions 1 and 2 described above. It would also apply for condition 3 if the **servers-unreachable** command is not configured. But, if configured it would take the highest precedence for all Diabase errors scenarios.

This command can also be used to control the triggering of behavior based on either due to transport failure, response message timeouts or Tx expiry when OCS becomes unreachable. The transport failure could be due to no TCP connection and the message timeout could be due to network congestion or any other network related issues.

The following are the possible and permissible configurations with respect to behavior triggering:

- **servers-unreachable behavior-triggers { initial-request | update-request } transport-failure**
- **servers-unreachable behavior-triggers { initial-request | update-request } transport-failure response-timeout**
- **servers-unreachable behavior-triggers { initial-request | update-request } transport-failure tx-expiry**

Of these configurations, the first one is considered to be the default configuration and it will take care of backward compatibility.

Example

The following command configures to terminate initial request calls if Diameter servers/OCS becomes unreachable after a timeout period of *1111* seconds:

```
servers-unreachable initial-request terminate after-timer-expiry 1111
```

timestamp-rounding

This command configures how to convert exact time into the units that are used in quotas.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
timestamp-rounding { ceiling | floor | roundoff }

default timestamp-rounding
```

default

Configures the default timestamp-rounding setting.
Default: **roundoff**

timestamp-rounding ceiling

Round off to the smallest integer greater than the fraction.
If the fractional part of the seconds is greater than 0, add 1 to the number of seconds and discard the fraction.

timestamp-rounding floor

Discard the fractional part of the second.

timestamp-rounding roundoff

Set the fractional part of the seconds to the nearest integer value. If the fractional value is greater than or equal to 0.5, add 1 to the number of seconds and discard the fractional part of second.

Usage

Use this command to configure how to convert exact time into the units that are used in quotas for CCA charging.
The specified rounding will be performed before system attempts any calculation. For example using round-off, if the start time is 1.4, and the end time is 1.6, then the calculated duration will be 1 (i.e., 2 – 1 = 1).

Example

The following command sets the CCA timestamp to nearest integer value second (for example, 34:12.23 to 34:12.00):

```
timestamp-rounding roundoff
```

trigger type

This command enables/disables triggering a credit reauthorization when the named values in the subscriber session changes.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] trigger type { cellid | lac | | mcc | mnc | qos | rat | serving-node | sgsn } +

default trigger type

default

Configures this command with the default setting.
Default: No triggers.

no

Removes the previously configured trigger type.

cellid

Sets the trigger based on change in cell identity or Service Area Code (SAC).

lac

Sets the trigger based on change in Location Area Code.

mcc

Sets the trigger based on change in Mobile Country Code (MCC).

mnc

Sets the trigger based on change in Mobile Network Code (MNC).

qos

Sets the trigger based on change in the Quality of Service (QoS).

rat

Sets the trigger based on change in the Radio Access Technology (RAT).

serving-node

Sets the trigger based on change in serving node. The serving node change causes the credit control client to ask for a re-authorization of the associated quota.
Typically used as an extension to sgsn trigger in P-GW, however, may also be used alone.

sgsn

Sets the trigger based on change in the IP address of SGSN.

+

Indicates that more than one of the previous keywords can be entered within a single command.

Usage

Use this command to set the credit control reauthorization trigger.

Example

The following command selects a credit control trigger as **lac**:

```
trigger type lac
```

usage-reporting

This command configures the ACS Credit Control usage reporting type.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
usage-reporting quotas-to-report based-on-grant { report-only-granted-volume }

default usage-reporting quotas-to-report
```

default

Configures this command with the default setting.
Default: Disabled

report-only-granted-volume

Suppresses the input and output octets. If the Granted-Service-Unit (GSU) AVP comes with CC-Total-Octets, then the device will send total, input and output octets in Used-Service-Unit (USU) AVP. If it comes with Total-Octets, the device will send only Total-Octets in USU.

Usage

Use this command to configure reporting usage only for granted quota. On issuing this command, the Used-Service-Unit AVP will report quotas based on grant i.e, only the quotas present in the Granted-Service-Unit AVP.
With this command only the units for which the quota was granted by the DCCA server will be reported irrespective of the reporting reason.

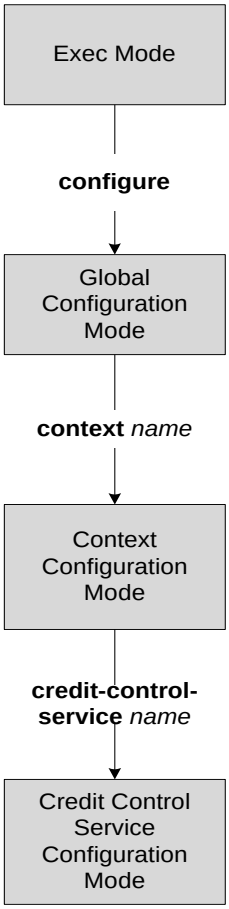
Example

The following command configures to report usage based only on granted quota:

```
usage-reporting quotas-to-report based-on-grant
```

Chapter 55
Credit Control Service Configuration Mode Commands

The Credit Control Service Configuration Mode is used to create and manage Credit Control Service.



diameter dictionary

This command configures the Diameter dictionary to be used for this Credit Control Service instance.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
diameter dictionary { custom1 | standard }

default diameter dictionary
```

default

Configures the default setting.

dictionary { custom1 | standard }

Specifies the Diameter dictionary to be used.
custom1: Specifies the custom dictionary **custom1**.
standard: Specifies the standard dictionary.

Usage

Use this command to configure the Diameter dictionary to be used for this Credit Control Service instance.

Example

The following command configures the standard Diameter dictionary:

```
diameter dictionary standard
```

diameter endpoint

This command configures the Diameter Credit Control Interface Endpoint.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter endpoint *endpoint_name*

{ default | no } diameter endpoint

default

Configures the default setting.

no

Removes the previous Diameter endpoint configuration.

endpoint_name

Specifies the Diameter endpoint name as an alpha and/or numeric string of 1 through 63 characters.

Usage

Use this command to configure the Diameter Credit Control Interface Endpoint.

Example

The following command configures the Diameter Credit Control Interface Endpoint named *test135*:

```
diameter endpoint test135
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

failure-handling

This command configures the Diameter failure handling behavior.

Product

All

Privilege

Security Administrator, Administrator

Syntax

failure-handling { initial-request | terminate-request | update-request } { diameter-result-code *result_code* **[to** *result_code* **] | peer-unavailable | request-timeout } action { continue | retry-and-continue | retry-and-terminate | terminate }**

{ default | no } failure-handling { initial-request | terminate-request | update-request } { diameter-result-code *result_code* **[to** *result_code* **] | peer-unavailable | request-timeout }**

default

Configures the default setting.

no

Removes the previous failure handling configuration.

initial-request | terminate-request | update-request

initial-request: Specifies failure handling for Initial Request.
terminate-request: Specifies failure handling for Terminate Request.
update-request: Specifies failure handling for Update Request.

diameter-result-code | peer-unavailable | request-timeout

diameter-result-code *result_code* **[to** *result_code* **]**: Specifies Diameter result code(s) for failure handling.
result_code must be an integer from 3000 through 9999.
to *result_code*: Specifies the range of Diameter result codes.
peer-unavailable: Specifies failure handling for peer being unavailable.
request-timeout: Specifies failure handling for request timeouts.

action { continue | retry-and-continue | retry-and-terminate | terminate }

Specifies the failure handling action.
continue: Continue the session without credit control.
retry-and-continue: Retry and, even if credit control is not available, continue.
retry-and-terminate: Retry and then terminate.
terminate: Terminate the session.

Usage

Use this command to configure the Diameter failure handling behavior.

Example

The following command configures initial request failure handling behavior for Diameter result codes *3001* to *4001* with terminate action:

```
failure-handling initial-request diameter-result-code 3001 to 4001 action
terminate
```

request timeout

This command configures the timeout period for Diameter requests.

Product

All

Privilege

Security Administrator, Administrator

Syntax

request timeout *timeout*

{ default | no } request timeout

default

Configures the default setting.

no

Removes the previous request timeout configuration.

timeout

Specifies the timeout period in seconds. The value must be an integer from 1 through 300.

Usage

Use this command to configure the Diameter request timeout value, after which the request is deemed to have failed. This timeout is an overall timeout, and encompasses all retries with the server(s).

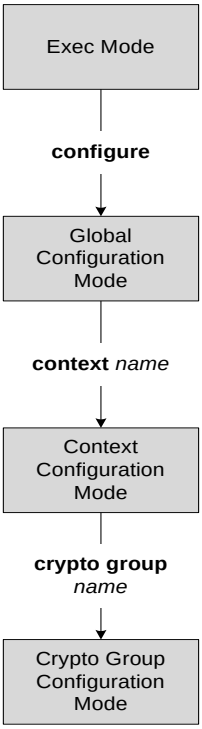
Example

The following command configures the timeout period to *150* seconds:

```
request timeout 150
```

Chapter 56
Crypto Group Configuration Mode Commands

The Crypto Group Configuration Mode is used to configure crypto (tunnel) groups that provide fail-over redundancy for IPSec tunnels to packet data networks (PDNs).



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

match address

Associates an access control list (ACL) with the crypto group.

Product

PDSN, HA, GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

[no] match address *acl_name* **[** *preference* **]**

no

Deletes a previously configured ACL association.

match address *acl_name*

Specifies the name of the ACL being matched to the crypto group entered as an alphanumeric string of 1 through 47 characters.

preference

The priority of the ACL.
The ACL preference is factored when a single packet matches the criteria of more than one ACL.
preference is an integer from 0 through 4294967295; 0 is the highest priority.
If multiple ACLs are assigned the same priority, the last one entered will be used first.

Important: The priorities are only compared for ACLs matched to other groups or to policy ACLs (those applied to the entire context).

Usage

IP ACLs are associated with crypto groups using this command. Both the crypto group and the ACLs must be configured in the same context.
ISAKMP crypto maps can then be associated with the crypto group. This allows user traffic matching the rules of the ACL to be handled according to the policies configured as part of the crypto map.

Example

The following command associates an ACL called *corporate_acl* to the crypto group:

```
match address corporate_acl
```

match ip pool

Matches the specified IP pool to the current crypto group. This command can be used multiple times to match more than one IP pool.

Product

PDSN, HA, GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

[no] match ip pool pool-name *pool_name*

no

Deletes the matching statement for the specified IP pool from the crypto group.

match ip pool pool-name *pool_name*

Specifies the name of an existing IP pool that should be matched entered as an alphanumeric string of 1 through 31 characters.

Usage

Use this command to set the names of IP pools that should be matched in the current crypto group.

Example

The following command sets a rule for the current crypto group that will match an IP pool named *ippool1*:

```
match ip pool pool-name ippool1
```

switchover

Configures the fail-over properties for the crypto group as part of the Redundant IPSec Fail-Over feature.

Product

PDSN, HA, GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] switchover auto [ do-not-revert ]
```

no

Disables the automatic switchover of tunnels. This applies to switching primary-to-secondary and secondary-to-primary.

switchover auto

Allows the automatic switchover of tunnels. Default: Enabled

do-not-revert

Disables the automatic switchover of secondary tunnels to primary tunnels. Default: Disabled

Usage

This command configures the fail-over options for the Redundant IPSec Fail-over feature.
If the automatic fail-over options are disabled, tunneled traffic must be manually switched to the alternate tunnel (or manually activated if no alternate tunnel is configured and available) using the following command in the Exec Mode:

```
crypto-group group_name activate { primary | secondary }
```

For a definition of this command, see the **crypto-group** section of the Exec Mode Commands chapter of this guide.

Example

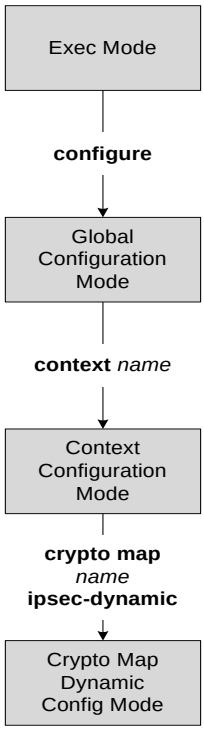
The following command disables the automatic secondary-to-primary switchover:

```
switchover auto do-not-revert
```

Chapter 57
Crypto Map Dynamic Configuration Mode Commands

The Crypto Map Dynamic Configuration Mode is used to configure IPSec tunnels that are created as needed to facilitate subscriber sessions using Mobile IP or L2TP.

Modification(s) to an existing dynamic crypto map configuration will not take effect until the related security association has been cleared. Refer to the description of the **`clear crypto security-association`** command in the *Exec Mode Commands* chapter for more information.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

set

Configures parameters for the dynamic crypto map.

Product

PDSN, HA, GGSN, PDIF

Privilege

Security Administrator, Administrator

Syntax

set { control-dont-fragment { clear-bit | copy-bit | set-bit } | isakmp natt [keepalive *time* **] | pfs { group1 | group2 | group5} | phase1-idtype { id-key-id | ipv4-address } [mode { aggressive | main }] | phase2-idtype { ipv4-address | ipv4-address-subnet} | security-association lifetime { keepalive | kilo-bytes** *kbytes* **| seconds** *secs* **} | transform-set** *transform_name* **[transform-set** *transform_name2 ...* **transform-set** *transform_name6* **] }**
no set { pfs | security-association lifetime {keepalive | kilo-bytes | seconds } | phase1-idtype | phase2-idtype | transform-set *transform_name* **[transform-set** *transform_name2 ...* **transform-set** *transform_name6* **] }**

---

no

Deletes the specified parameter or resets the specified parameter to the default value.

---

control-dont-fragment { clear-bit | copy-bit | set-bit }

Controls the don't fragment (DF) bit in the outer IP header of the IPSec tunnel data packet. Options are:

- **clear-bit**: Clears the DF bit from the outer IP header (sets it to 0).
- **copy-bit**: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
- **set-bit**: Sets the DF bit in the outer IP header (sets it to 1).

---

isakmp natt [keepalive *time* **]**

Enable IPSec NAT Traversal.
keepalive *time*: The time to keep the NAT connection alive in seconds. *time* must be an integer of from 1 through 3600.

---

pfs { group1 | group2 | group5 }

Specifies the modp Oakley group (also known as the Diffie-Hellman [D-H] group) that is used to determine the length of the base prime numbers that are used for Perfect Forward Secrecy (PFS).

- **group1**: Diffie-Hellman Group1 (768-bit modp)
- **group2**:- Diffie-Hellman Group2 (1024-bit modp)
- **group5**:- Diffie-Hellman Group5 (1536-bit modp)

---

phase1-idtype { id-key-id | ipv4-address } [mode { aggressive | main }]

Sets the IKE negotiations Phase 1 payload identifier.
Default: ipv4-address

id-key-id: Use ID_KEY_ID as the Phase 1 payload identifier.
ipv4-address: Use IPV4_ADDR as the Phase 1 payload identifier.
mode { aggressive | main }: Specify the IKE mode.

---

phase2-idtype { ipv4-address | ipv4-address-subnet }

Sets the IKE negotiations Phase 2 payload identifier.
Default: ipv4-address-subnet
ipv4-address: Use IPV4_ADDR as the Phase 2 payload identifier.
ipv4-address-subnet: Use IPV4_ADDR_SUBNET as the Phase 2 payload identifier.

---

security-association lifetime { keepalive | kilo-bytes *kbytes* **| seconds** *secs* **}**

Defaults:

- **keepalive**: Disabled
- **kilo-bytes**: 4608000 kbytes
- **seconds**: 28800 seconds

This keyword specifies the parameters that determine the length of time an IKE Security Association (SA) is active when no data is passing through a tunnel. When the lifetime expires, the tunnel is torn down. Whichever parameter is reached first expires the SA lifetime.

- **keepalive**: The SA lifetime expires only when a keepalive message is not responded to by the far end.
- **kilo-bytes**: This specifies the amount of data in kilobytes to allow through the tunnel before the SA lifetime expires; entered as an integer from 2560 through 4294967294.
- **seconds**: The number of seconds to wait before the SA lifetime expires; entered as an integer from 1200 through 86400.

Important: If the dynamic crypto map is being used in conjunction with Mobile IP and the Mobile IP renewal timer is less than the crypto map's SA lifetime (either in terms of kilobytes or seconds), then the **keepalive** parameter **must** be configured.

---

transform-set *transform_name* **[transform-set** *transform_name2 ...* **transform-set** *transform_name6* **]**

Specifies the name of a transform set configured in the same context that will be associated with the crypto map. Refer to the command **crypto ipsec transform-set** for information on creating transform sets. You can repeat this keyword up to 6 times on the command line to specify multiple transform sets. *trasnform_name* is the name of the transform set entered as an alphanumeric string from 1 through 127 characters that is case sensitive.

Usage

Use this command to set parameters for a dynamic crypto map.

Example

The following command sets the PFS group to Group1:

```
set pfs group1
```

The following command sets the SA lifetime to *50000* KB:

```
set security-association lifetime kilo-bytes 50000
```

The following command sets the SA lifetime to *10000* seconds:

```
set security-association lifetime seconds 10000
```

The following command enables the SA to re-key when the tunnel lifetime expires:

```
set security-association lifetime keepalive
```

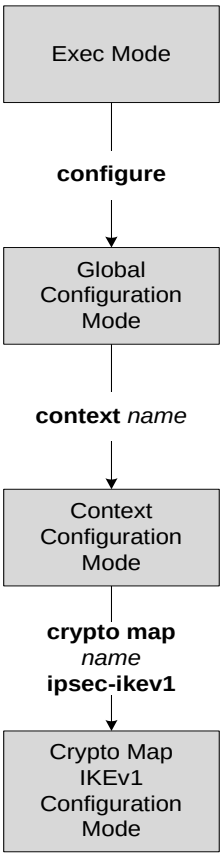
The following command defines transform sets *tset1* and *tset2*:

```
set transform-set tset1 transform-set tset2
```

Chapter 58
Crypto Map IKEv1 Configuration Mode Commands

The Crypto Map IKEv1 Configuration Mode is used to configure properties for IPSec tunnels that will be created using the Internet Key Exchange (IKE) that operates within the framework of the Internet Key Exchange version 1 (IKEv1).

Modification(s) to an existing IKEv1 crypto map configuration will not take effect until the related security association has been cleared. Refer to the description of the **`clear crypto security-association`** command in the *Exec Mode Commands* chapter for more information.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

match address

Matches or associates the crypto map to an access control list (ACL) configured in the same context.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

[no] match address *acl_name priority*

no

Removes a previously matched ACL.

match address *acl_name*

Specifies the name of the ACL with which the crypto map is to be matched as an alphanumeric string of 1 through 79 characters that is case sensitive.

priority

Specifies the preference of the ACL. The ACL preference is factored when a single packet matches the criteria of more than one ACL.
The preference is an integer value from 0 to 4294967295; 0 is the highest priority. Default: 0

Important: The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).

Usage

ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel.
Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

Example

The following command sets the crypto map ACL to the ACL named *ACLlist1* and sets the crypto maps priority to the highest level.

```
match address ACLlist1 0
```

match crypto group

Matches or associates the crypto map a crypto group configured in the same context.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

[no] match crypto group *group_name* **{ primary | secondary }**

no

Deletes a previously configured crypto group association.

match crypto group *group_name*

Specifies the name of the crypto group entered as an alphanumeric string of 1 through 127 characters that is case sensitive.

primary

Specifies that the policies configured as part of this crypto map will be used for the primary tunnel in the Redundant IPSec Tunnel Failover feature.

secondary

Specifies that the policies configured as part of this crypto map will be used for the secondary tunnel in the Redundant IPSec Tunnel Failover feature.

Usage

Use this command to dictate the primary and secondary tunnel policies used for the Redundant IPSec Tunnel Failover feature.
At least two policies must be configured to use this feature. One policy must be configured as the primary, the other as the secondary.

Example

The following command associates the crypto map to a crypto group called *group1* and dictates that it will serve as the primary tunnel policy:

```
match crypto group group1 primary
```

match ip pool

Matches the specified IP pool to the current IKEv1 crypto map. This command can be used multiple times to change more than one IP pool.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

[no] match ip pool pool-name *pool_name*[**destination-network** *ip_address* **{ /** *mask* **| mask** *ip_mask* **}]**

no

Delete the matching statement for the specified IP pool from the crypto map.

match ip pool pool-name *pool_name*

Specifies the name of an existing IP pool that should be matched as an alphanumeric string of 1 through 31 characters.

destination-network *ip_address* **{ /** *mask* **| mask** *ip_mask* **}**

Specifies the IP address of the destination network in IPv4 dotted-decimal notation.
/mask specifies the subnet mask bits (representing the subnet mask) and must be an integer from 1 to 32 (CIDR notation). This variable must be entered in theIPv4 dotted-decimal notation/subnet bits format (for example, 10.1.1.1/24).
mask *ip_mask* specifies the subnet mask in dotted decimal notation.
An IP pool attached to the crypto map can have multiple IPSec tunnels according to the destination of the packet being forwarded to internet.

Important: Each invocation of this command will add another destination network to the IP pool, with a maximum of eight destination networks per crypto map.

Usage

Use this command to set the names of IP pools that should be matched in the current crypto map.

Important: If an IP address pool that is matched to a IKEv1 crypto map is resized, removed, or added, the corresponding security association must be cleared in order for the change to take effect. Refer to the **clear crypto** command in the Exec mode for information on clearing security associations.

Example

The following command sets a rule for the current crypto map that will match an IP pool named *ippool1*:

```
match ip pool pool-name ippool1
```

set

Configures parameters for the dynamic crypto map.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

set { control-dont-fragment { clear-bit | copy-bit | set-bit } | ikev1 natt [keepalive *time* **] | pfs { group1 | group2 | group5 } | phase1-idtype { id-key-id | ipv4-address [mode { aggressive | main }] | phase2-idtype { ipv4-address | ipv4-address-subnet } | security-association lifetime { disable-phase2-rekey | keepalive | kilo-bytes** *kbytes* **| seconds** *secs* **} transform-set** *transform_name* **[transform-set** *transform_name2 ...* **transform-set** *transform_name6* **]**
no set { ikev1 natt | pfs | phase1-idtype | phase2-idtype | security-association lifetime { disable-phase2-rekey | keepalive | kilo-bytes | seconds } | transform-set *transform_name* **[transform-set** *transform_name2 ...* **transform-set** *transform_name6* **]**

---

set control-dont-fragment { clear-bit | copy-bit | set-bit }

Controls the don't fragment (DF) bit in the outer IP header of the IPsec tunnel data packet. Options are:

- **clear-bit**: Clears the DF bit from the outer IP header (sets it to 0).
- **copy-bit**: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
- **set-bit**: Sets the DF bit in the outer IP header (sets it to 1).

---

set ikev1 natt [keepalive *time* **]**

Specifies IKE parameters.
natt: Enables IPSec NAT Traversal.
keepalive *time*: The time to keep the NAT connection alive in seconds. *time* must be an integer of from 1 through 3600.

---

set pfs { group1 | group2 | group5 }

Specifies the modp Oakley group (also known as the Diffie-Hellman [D-H] group) that is used to determine the length of the base prime numbers that are used for Perfect Forward Secrecy (PFS).

- **group1**: Diffie-Hellman Group1 (768-bit modp)
- **group2**: Diffie-Hellman Group2 (1024-bit modp)
- **group5**: Diffie-Hellman Group5 (1536-bit modp)

---

set phase1-idtype { id-key-id | ipv4-address [mode { aggressive | main }]

Sets the IKE negotiations Phase 1 payload identifier. Default: id-key-id
id-key-id: ID KEY ID
ipv4-address: ID IPV4 Address

- **mode**: Configures IKE mode
- **aggressive**: IKE negotiation mode: AGGRESSIVE

- **main**: IKE negotiation mode: MAIN

set phase2-idtype { ipv4-address | ipv4-address-subnet }

Sets the IKE negotiations Phase 2 payload identifier.
Default: ipv4-address-subnet

- **ipv4-address**: Use IPV4_ADDR as the Phase 2 payload identifier.
- **ipv4-address-subnet**: Use IPV4_ADDR_SUBNET as the Phase 2 payload identifier.

set security-association lifetime { disable-phase2-rekey | keepalive | kilo-bytes *kbytes* **| seconds** *secs* **}**

Defaults:

- **disable-phase2-rekey**: Rekeying is enabled by default
- **keepalive**: Disabled
- **kilo-bytes:** 4608000 kbytes
- **seconds:** 28800 seconds

Specifies the parameters that determine the length of time an IKE Security Association (SA) is active when no data is passing through a tunnel. When the lifetime expires, the tunnel is torn down. Whichever parameter is reached first expires the SA lifetime.

- **disable-phase2-rekey**: If this keyword is specified, the Phase2 SA is not rekeyed when the lifetime expires.
- **keepalive**: The SA lifetime expires only when a keepalive message is not responded to by the far end.
- **kilo-bytes**: This specifies the amount of data (n kilobytes) to allow through the tunnel before the SA lifetime expires. *kbytes* must be an integer from 2560 through 4294967294.
- **set seconds**: The number of seconds to wait before the SA lifetime expires. *secs* must be an integer from 1200 through 86400.

Important: If the dynamic crypto map is being used in conjunction with Mobile IP and the Mobile IP renewal timer is less than the crypto map's SA lifetime (either in terms of kilobytes or seconds), then the keepalive parameter must be configured.

transform-set *transform_name* **[transform-set** *transform_name2* **... transform-set** *transform_name6* **]**

Specifies the name of a transform set configured in the same context that will be associated with the crypto map. Refer to the command **crypto ipsec transform-set** for information on creating transform sets. You can repeat this keyword up to 6 times on the command line to specify multiple transform sets. *transform_name* is the name of the transform set entered as an alphanumeric string of 1 through 127 characters that is case sensitive.

no

Deletes the specified parameter or resets the specified parameter to the default value.

Usage

Use this command to set parameters for a dynamic crypto map.

Example

The following command sets the PFS group to Group1:

```
set pfs group1
```

The following command sets the SA lifetime to *50000* KB:

```
set security-association lifetime kilo-bytes 50000
```

The following command sets the SA lifetime to *10000* seconds:

```
set security-association lifetime seconds 10000
```

The following command enables the SA to re-key when the tunnel lifetime expires:

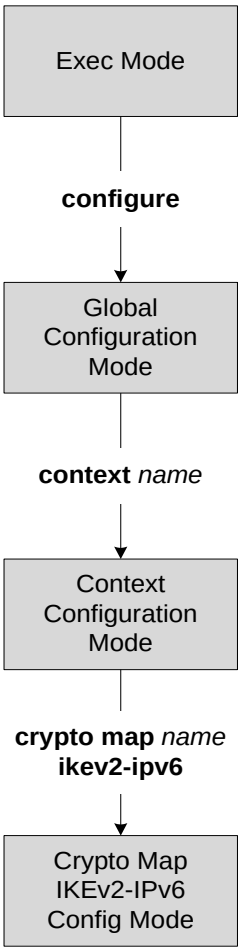
```
set security-association lifetime keepalive
```

The following command defines transform sets *tset1* and *tset2*.

```
set transform-set tset1 transform-set tset2
```

Chapter 59
Crypto Map IKEv2-IPv6 Configuration Mode Commands

The Crypto Map IKEv2-IPv6 Configuration Mode is used to configure an IKEv2 IPsec policy for secure X3 interface tunneling between a P-GW and a lawful intercept server.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

authentication

Configures the subscriber authentication method used for the P-GW lawful intercept service.

Product

P-GW

Privilege

Administrator

Syntax

authentication pre-shared-key { encrypted key *value* **| key** *value* **}**

---

authentication pre-shared-key { encrypted key *value* **| key** *value* **}**

Specifies that a pre-shared key is to be used for authenticating a subscriber in the PDIF service.
encrypted key *value*: Specifies that the pre-shared key used for authentication is encrypted and expressed as an alphanumeric string of 1 through 255 characters.
key *value*: Specifies that the pre-shared key used for authentication is clear text and expressed as an alphanumeric string of 1 through 255 characters.

Usage

Use this command to specify the type of authentication performed for subscribers attempting to access the P-GW service using this crypto map.

Example

The following command sets the authentication method to an open key value of *6d79706173737 6f7264*:

```
authentication pre-shared-key key 6d79706173737 6f7264
```

control-dont-fragment

Controls the Don't Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

Product

P-GW

Privilege

Administrator

Syntax

```
control-dont-fragment { clear-bit | copy-bit | set-bit }
```

{ clear-bit | copy-bit | set-bit }

clear-bit: Clears the DF bit from the outer IP header (sets it to 0).
copy-bit: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
set-bit: Sets the DF bit in the outer IP header (sets it to 1).

Usage

A packet is encapsulated in IPsec headers at both ends. The new packet can copy the DF bit from the original unencapsulated packet into the outer IP header, or it can set the DF bit if there is not one in the original packet. It can also clear a DF bit that it does not need.

Example

The following command sets the DF bit in the outer IP header:

```
control-dont-fragment set-bit
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

ikev2-ikesa

Configures parameters for the IKEv2 IKE Security Associations within this crypto template.

Product

P-GW

Privilege

Administrator

Syntax

ikev2-ikesa { max-retransmissions *number* **| rekey | setup-timer** *sec* **}**

default ikev2-ikesa { max-retransmissions | rekey | setup-timer }

no ikev2-ikesa rekey

default

Restores the selected keyword to its default value.

no ikev2-ikesa

Disables a previously enabled parameter.

ikev2-ikesa max-retransmissions *number*

Specifies the maximum number of retransmissions of an IKEv2 IKE exchange request if a response has not been received. *number* must be an integer from 1 to 8. Default: 5

ikev2-ikesa rekey

Specifies if IKESA rekeying should occur before the configured lifetime expires (at approximately 90% of the lifetime interval). Default is not to re-key.

ikev2-ikesa setup-timer *sec*

Specifies the number of seconds before an IKEv2 IKE Security Association that is not fully established is terminated. *sec* must be an integer from 1 to 3600. Default: 60

Usage

Use this command to configure parameters for the IKEv2 IKE Security Associations within this crypto template.

Example

The following command configures the maximum number of IKEv2 IKESA request retransmissions to 7:

```
ikev2-ikesa max-retransmissions 7
```

match

Matches or associates the crypto map to an access control list (ACL) configured in the same context.

Product

P-GW

Privilege

Administrator

Syntax

match address *acl_name* **[** *priority* **]**

no match address

no

Removes a previously matched ACL.

match address *acl_name*

Specifies The name of the ACL with which the crypto map is to be matched. *acl_name* is an alphanumeric string of 1 through 79 characters that is case sensitive.

priority

Specifies the preference of the ACL as integer from 0 through 4294967295. 0 is the highest priority. Default: 0
The ACL preference is factored when a single packet matches the criteria of more than one ACL.

Important: The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).

Usage

ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel.
Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

Example

The following command sets the crypto map ACL to the ACL named *acl-list1* and sets the crypto maps priority to the highest level.

```
match address acl-list1 0
```

payload

Creates a new, or specifies an existing, crypto template payload and enters the Crypto Template Payload Configuration Mode.

Product

P-GW

Privilege

Administrator

Syntax

payload *name* **match ipv6**

no payload *name*

payload *name*

Specifies the name of a new or existing crypto template payload as an alphanumeric string of 1 through 127 characters.

match ipv6

Filters IPSec IPv6 Child Security Association creation requests for subscriber calls using this payload. Further filtering can be performed by applying the following:

Usage

Use this command to create a new or enter an existing crypto template payload. The payload mechanism is a means of associating parameters for the Security Association (SA) being negotiated.
Two payloads are required: one each for MIP and IKEv2. The first payload is used for establishing the initial Child SA Tunnel Inner Address (TIA) which will be torn down. The second payload is used for establishing the remaining Child SAs. Note that if there is no second payload defined with home-address as the *ip-address-allocation* then no MIP call can be established, just a Simple IP call.
Currently, the only available match is for ChildSA, although other matches are planned for future releases.
Entering this command results in the following prompt:
[*ctxt_name*]*hostname*(cfg-crypto-<*name*>-ikev2-tunnel-payload)#
Crypto Template IKEv2-IPv6 Payload Configuration Mode commands are defined in the Crypto Template IKEv2-IPv6 Payload Configuration Mode Commands chapter.

Example

The following command configures a crypto template payload called *payload5* and enters the Crypto Template IKEv2-IPv6 Payload Configuration Mode:

```
payload payload5 match ipv6
```

peer

Configures the IP address of a peer IPSec server.

Product

P-GW

Privilege

Administrator

Syntax

peer *ip_address*

no peer

no

Removes the configured peer server IP address.

peer *ip_address*

Specifies the IP address of a peer IPSec server in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to specify a peer IPsec peer server. The IPsec peer server can also be the Lawful Intercept server.

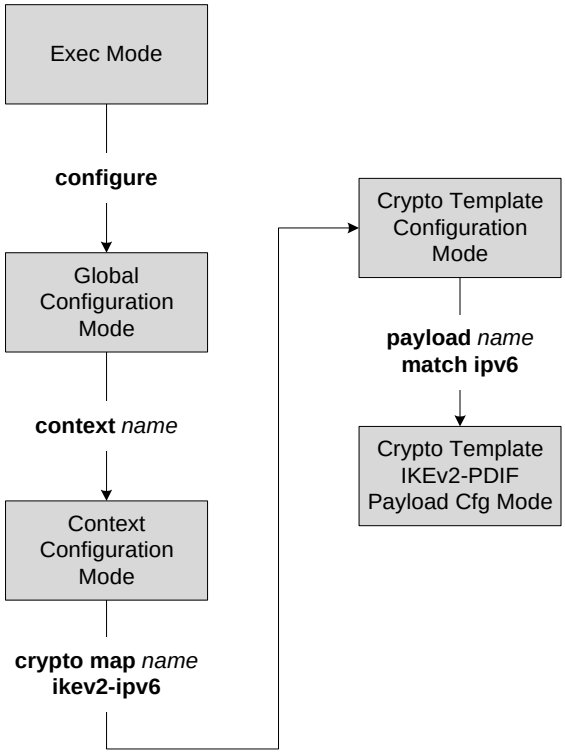
Example

The following command configures the system to recognize an IPsec peer server with an IPv6 address of *fe80::200:f8ff:fe21:67cf*:

```
peer fe80::200:f8ff:fe21:67cf
```

Chapter 60
Crypto Map IKEv2-IPv6 Payload Configuration Mode Commands

The Crypto Map IKEv2-IPv6 Payload Configuration Mode is used to assign the correct IPSec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

ipsec

Configures the IPSec transform set to be used for this crypto template payload.

Product

P-GW

Privilege

Administrator

Syntax

ipsec transform-set list *name*

no ipsec transform-set list

ipsec transform-set list *name*

Specifies the context configured IPSec transform set name to be used in the crypto template payload. This is a space-separated list. From 1 to 4 transform sets can be entered. *name* is an alphanumeric string of 1 through 127 characters.

Usage

Use this command to list the IPSec transform set(s) to use in this crypto template payload.

Example

The following command configures IPSec transform sets named *ipset1* and *ipset2* to be used in this crypto template payload:

```
ipsec transform-set list ipset1 ipset2
```

lifetime

Configures the number of seconds for IPSec Child SAs derived from this crypto template payload to exist.

Product

P-GW

Privilege

Administrator

Syntax

lifetime *sec* **[kilo-bytes** *kbytes* **]**

default lifetime

default

Returns the lifetime value to the default setting of 86400.

lifetime *sec*

Specifies the number of seconds for IPSec Child Security Associations derived from this crypto template payload to exist. *sec* must be an integer from 60 through 604800. Default: 86400

kilo-bytes *kbytes*

Specifies lifetime in kilo-bytes for IPSec Child Security Associations derived from this Crypto Map. *kbytes* must be an integer from 1 through 2147483648.

Usage

Use this command to configure the number of seconds for IPSec Child Security Associations derived from this crypto template payload to exist.

Example

The following command configures the IPSec child SA lifetime to be 120 seconds:

```
lifetime 120
```

rekey

Configures child security association rekeying.

Product

P-GW

Privilege

Administrator

Syntax

```
rekey [ keepalive ]

[ default | no ] rekey
```

default

Returns the feature to the default setting of disabled.

no

Disables this feature.

keepalive

If specified, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default rekeying is only performed if there has been data exchanged since the previous rekey.

Usage

Use this command to enable or disable the ability to rekey IPSec Child SAs after approximately 90% of the Child SA lifetime has expired. The default, and recommended setting, is not to perform rekeying. No rekeying means the PDIF will not originate rekeying operations and will not process CHILD SA rekeying requests from the MS.

Example

The following command disables rekeying:

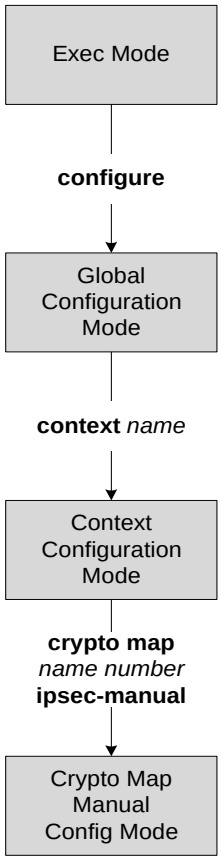
```
no rekey
```

Chapter 61
Crypto Map Manual Configuration Mode Commands

The Crypto Map Manual Configuration Mode is used to configure static IPSec tunnel properties.

Modification(s) to an existing crypto map manual configuration will not take effect until the related security association has been cleared. Refer to the description of the **`clear crypto security-association`** command in the *Exec Mode Commands* chapter for more information.

Important: Because manual crypto map configurations require the use of static security keys (associations), they are not as secure as crypto maps that rely on dynamically configured keys. Therefore, they only be used for testing purposes.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

match address

Matches or associates the crypto map to an access control list (ACL) configured in the same context.

Product

PDSN, HA, GGSN, PDIF

Privilege

Security Administrator, Administrator

Syntax

[no] match address *acl_name* **[** *priority* **]**

no

Removes a previously matched ACL.

match address *acl_name*

Specifies the name of the ACL with which the crypto map is to be matched. *acl_name* is an alphanumeric string of 1 through 47 characters that is case sensitive.

priority

Specifies the preference of the ACL. The ACL preference is factored when a single packet matches the criteria of more than one ACL. *priority* is an integer from 0 through 4294967295. 0 is the highest priority. Default: 0

Important: The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).

Usage

ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel.
Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

Example

The following command sets the crypto map ACL to the ACL named *ACLlist1* and sets the crypto maps priority to the highest level.

```
match address ACLlist1 0
```

set control-dont-fragment

Controls the Don't Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

Product

PDSN, HA, GGSN, PDIF

Privilege

Security Administrator, Administrator

Syntax

```
set control-dont-fragment { clear-bit | copy-bit | set-bit }

default set control-dont-fragment { clear-bit | copy-bit | set-bit }
```

default

Sets or restores default value assigned to a specified parameter.

set control-dont-fragmentclear-bit

Clears the DF bit from the outer IP header (sets it to 0).

set control-dont-fragmentcopy-bit

Copies the DF bit from the inner IP header to the outer IP header. This is the default action.

set control-dont-fragmentset-bit

Sets the DF bit in the outer IP header (sets it to 1).

Usage

Use this command to clear, copy, or set the don't fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

Example

The following command sets the DF bit in the outer IP header.

```
set control-dont-fragment set-bit
```

set peer

Configures the IP address of the peer security gateway that the system will establish the IPSec tunnel with.

Product

PDSN, HA, GGSN, PDIF

Privilege

Security Administrator, Administrator

Syntax

[no] set peer *gw_address*

no

Removes a previously configured peer address.

set peer *gw_address*

Specifies the IP address of the peer security gateway with which the IPSec tunnel will be established.

Usage

Once the manual crypto map is fully configured and applied to an interface, the system will establish an IPSec tunnel with the security gateway specified by this command.
Because the tunnel relies on statically configured parameters, once created, it never expires; it exists until its configuration is deleted.

Example

The following command configures a security gateway address of *192.168.1.100* for the crypto map with which to establish a tunnel.

```
set peer 192.168.1.100
```

set session-key

Configures session key parameters for the manual crypto map.

Product

PDSN, HA, GGSN, PDIF

Privilege

Security Administrator, Administrator

Syntax

set session-key { inbound | outbound } { ah *ah_spi* **[encrypted] key** *ah_key* **| esp** *esp_spi* **[encrypted] cipher** *encryption_key* **[encrypted] authenticator** *auth_key* **}**
no set session-key { inbound | outbound }

---

no

Removes previously configured session key information.

---

inbound

Specifies that the key(s) will be used for tunnels carrying data sent by the security gateway.

---

outbound

Specifies that the key(s) will be used for tunnels carrying data sent by the system.

---

ah *ah_spi*

Configures the Security Parameter Index (SPI) for the Authentication Header (AH) protocol. The SPI is used to identify the AH security association (SA) between the system and the security gateway. *ah_spi* is an integer from 256 through 4294967295.

---

encrypted

Indicates the key provided is encrypted.
The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **key**, **cipher**, and/or **authenticator** keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

---

key *ah_key*

Configures the key used by the system to de/encapsulate IP packets using Authentication Header (AH) protocol. *ah_key* must be entered as either an alphanumeric string or a hexadecimal number beginning with "0x".
The length of the configured key must match the configured algorithm.

---

esp *esp_spi*

Configures SPI for the Encapsulating Security Payload (ESP) protocol. The SPI is used to identify the ESP security association (SA) between the system and the security gateway. *esp_spi* is an integer from 256 through 4294967295.
The length of the configured key must match the configured algorithm.

cipher *encryption_key*

Specifies the key used by the system to de/encrypt the payloads of IP packets using the ESP protocol. *encryption_key* must be entered as either an alphanumeric string or a hexadecimal number beginning with "0x".
The length of the configured key must match the configured algorithm.

authenticator *auth_key*

Specifies the key used by the system to authenticate the IP packets once encryption has been performed. *auth_key* must be entered as either an alphanumeric string or a hexadecimal number beginning with "0x".
The length of the configured key must match the configured algorithm.

Usage

Manual crypto maps rely on the use of statically configured keys to establish IPSec tunnels. This command allows the configuration of the static keys.
Identical keys must be configured on both the system and the security gateway in order for the tunnel to be established.
The length of the configured key must match the configured algorithm.
This command can be entered up to two time for the same crypto map: once to configure inbound key properties, and once to configure outbound key properties.

Example

The following command configures a manual crypto map with the following session key properties:

- Keys are for tunnels initiated by the system to the security gateway.
- ESP will be used with an SPI of *310*.
- Encryption key is *sd23r9skd0fi3as*.
- Authentication key is *sfd23408imi9yn*.

```
set session-key outbound esp 310 cipher sd23r9skd0fi3as authenticator
sfd23408imi9yn
```

set transform-set

Configures the name of a transform set that the crypto map is associated with.

Product

PDSN, HA, GGSN, PDIF

Privilege

Security Administrator, Administrator

Syntax

[no] set transform-set *transform_name*

no

Removes a previously configured transform set association.

set transform-set *transform_name*

Specifies the name of the transform set expressed as an alphanumeric string of 1 through 127 characters that is case sensitive.

Usage

System transform sets contain the IPSec policy definitions for crypto maps. Refer to the **crypto ipsec transform-set** command for information on creating transform sets.

Important: Transform sets must be configured prior to configuring session key information for the crypto map.

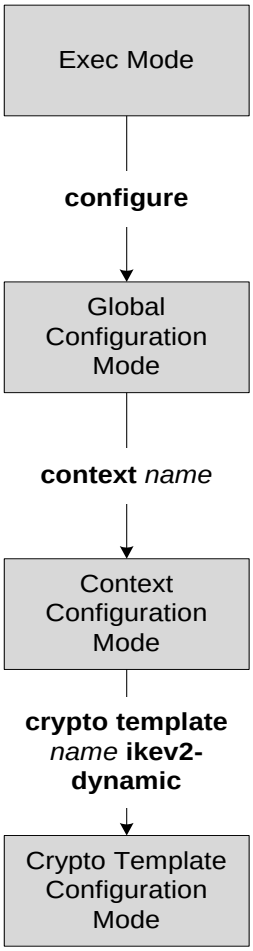
Example

The following command associates a transform set named *esp_tset* with the crypto map:

```
set transform-set esp_tset
```

Chapter 62
Crypto Template Configuration Mode Commands

The Crypto Template Configuration Mode is used to configure an IKEv2 IPSec policy. It includes most of the IPSec parameters and IKEv2 parameters for cryptographic and authentication algorithms. A security gateway service will not function without a configured crypto template. Only one crypto template can be configured per service.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

authentication

Configures the authentication method used for services using the crypto template.

Product

All IPSec-related services

Privilege

Security Administrator, Administrator

Syntax

authentication { eap-profile *name* **[second-phase eap-profile** *name* **] | gateway { encrypted key** *value* **| key** *clear_text* **} | local { certificate | pre-shared-key { encrypted key** *value* **| key** *clear_text* **} | pre-shared-key { encrypted key** *value* **| key** *clear_text* **} | remote { certificate | eap-profile** *name* **[second-phase eap-profile** *name* **] | pre-shared-key { encrypted key** *value* **| key** *clear_text* **} }**

[default | no] authentication gateway

default

Returns the command to its default setting.

no

Removes the authentication gateway form the configuration.

no authentication [local | remote] pre-shared-key

Disables authentication for the local/remote pre-shared-key.

---

eap-profile *name* **[second-phase eap-profile** *name* **]**

Specifies that authentication is to be performed using a named Extensible Authentication Protocol (EAP) profile. *name* is an alphanumeric string of 1 through 127 characters. Entering this keyword places the CLI in the EAP Authentication Configuration Mode.
The **second-phase eap-profile** *name* is only required for installations using multiple authentications. *name* must be an alphanumeric string of 1 through 127 characters.

---

gateway { encrypted key *value* **| key** *clear_text* **}**

Specifies the pre-shared gateway key used for gateway authentication.
encrypted key *value*: Specifies that the pre-shared key used for authentication is encrypted. *value* must be an alphanumeric string of 1 through 255 characters.
key *clear_text*: Specifies that the pre-shared key used for authentication is clear text. *clear_text* must be an alphanumeric string of 1 through 255characters.

---

local { certificate | pre-shared-key { encrypted key *value* **| key** *clear_text* **}**

Specifies the local authentication method required for services using the crypto template.
certificate: Specifies that the certificate method of authentication must be used for services using the crypto template.
pre-shared-key { encrypted key *value* **| key** *clear_text* **}**: Specifies that a pre-shared key is to be used for services using the crypto template. **encrypted key** *value* configures an encrypted pre-shared key used for authentication. *value* must be an alphanumeric string of 1 through 255characters. **key**

clear_text configures a clear text pre-shared key used for authentication. *clear_text* must be an alphanumeric string of 1 through 255characters.

---

pre-shared-key { encrypted key *value* **| key** *clear_text* **}**

Specifies that a pre-shared key is to be used for services using the crypto template.
encrypted key *value*: Specifies that the pre-shared key used for authentication is encrypted. *value* must be an alphanumeric string of 1 through 255 characters.
key *clear_text*: Specifies that the pre-shared key used for authentication is clear text. *clear_text* must be an alphanumeric string of 1 through 255 characters.

---

remote { certificate | eap-profile *name* **[second-phase eap-profile** *name* **] | pre-shared-key { encrypted key** *value* **| key** *clear_text* **}**

Specifies the remote authentication method required for services using the crypto template.
certificate: Specifies that the certificate method of remote authentication must be used for services using the crypto template.
eap-profile *name* **[second-phase eap-profile** *name* **]**: Specifies that remote authentication is to be performed using a named EAP profile. *name* must be an alphanumeric string of 1 through 127 characters. Entering this keyword places the CLI in the EAP Authentication Configuration Mode.
The **second-phase eap-profile** *name* is only required for installations using multiple authentications. *name* must be an alphanumeric string of 1 through 127 characters.
pre-shared-key { encrypted key *value* **| key** *clear_text* **}**: Specifies that a pre-shared key is to be used for services using the crypto template. **encrypted key** *value* configures an encrypted pre-shared key used for authentication. *value* must be an alphanumeric string of 1 through 255 characters. **key** *value* configures a clear text pre-shared key used for authentication. *clear_text* must be an alphanumeric string of 1 through 255 characters.

Usage

Use this command to specify the type of authentication performed for subscribers or gateways attempting to access the service using this crypto template.
Entering the **authentication eap-profile** command results in the following prompt:
[*context_name*]*hostname*(cfg-crypto-tmpl-eap-key)#
EAP Authentication Configuration Mode commands are defined in the *EAP Authentication Configuration Mode Commands* chapter.

Example

The following command enables authentication via an EAP profile named *eap23* for subscribers using the service with this crypto template:

```
authentication eap-profile eap23
```

ca-certificate list

Used to bind an X.509 Certificate Authority (CA) root certificate to a crypto template.

Product

All

Privilege

Administrator

Syntax

ca-certificate list ca-cert-name *name***[ca-cert-name** *name* **]**

no ca-certificate

no

Removes a CA root certificate from the list.

ca-certificate list ca-cert-name *name*

Binds the named X.509 Certificate Authority (CA) root certificate to a crypto template. *name* is an alphanumeric string of 1 through 127 characters.

Usage

Used to bind an X.509 CA root certificate to a template.

Example

Use the following example to add a CA root certificate to a list:

```
ca-certificate list CA_list1
```

ca-crl list

Binds one or more Certificate Authority-Certificate Revocation Lists (CA-CRLs) to this crypto template.

Product

All

Privilege

Administrator

Syntax

ca-crl list ca-crl-name *name* **[ca-crl-name** *name* **] +**

no ca-crl

no

Removes the CA-CRL configuration from this template.

ca-crl list ca-crl-name *name*

Specifies the CA-CRL to associate with this crypto template. *name* must be the name of an existing CA-CRL expressed as an alphanumeric string of 1 through 129 characters. Multiple lists can be configured for a crypto template.

Usage

Use this command to associate a CA-CRL name with this crypto template.
CA-CRLs are configured in the Global Configuration Mode. For more information about configuring CA-CRLs, refer to the **ca-crl name** command in the *Global Configuration Mode Commands* chapter.

Example

The following example binds CA-CRLs named *CRL-5* and *CRL-7* to this crypto template:

```
ca-crl list ca-crl-name CRL-5 ca-crl-name CRL-7
```

certificate

Used to bind an X.509 trusted certificate to a crypto template.

Product

All

Privilege

Administrator

Syntax

[no] certificate name *name*

no

Removes any applied certificate or prevents the certificate from being included in the Auth Exchange response payload.

name *name*

Binds the named X.509 trusted certificate to a crypto template. *name* is an alphanumeric string of 1 through 127 characters.

Usage

Can be used to bind an X.509 certificate to a template, or include or exclude it from the Auth Exchange response payload.

Example

Use the following example to prevent a certificate from being included in the Auth Exchange payload:

```
no certificate
```

control-dont-fragment

Controls the Don't Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

Product

All

Privilege

Administrator

Syntax

```
control-dont-fragment { clear-bit | copy-bit | set-bit }
```

{ clear-bit | copy-bit | set-bit }

Configures the option to perform on the DF bit.

- **clear-bit**: Clears the DF bit from the outer IP header (sets it to 0).
- **copy-bit**: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
- **set-bit**: Sets the DF bit in the outer IP header (sets it to 1).

Usage

A packet is encapsulated in IPSec headers at both ends. The new packet can copy the DF bit from the original unencapsulated packet into the outer IP header, or it can set the DF bit if there is not one in the original packet. It can also clear a DF bit that it does not need.

Example

The following command sets the DF bit in the outer IP header:

```
control-dont-fragment set-bit
```

default

Restores the default values for the selected parameter.

Product

All

Privilege

Security Administrator, Administrator

Syntax

default { authentication gateway | certificate | dns-handling | dos cookie-challenge detect-dos-attack | ikev2-ikesa { ignore-rekeying-requests | keepalive-user-activity | max-retransmission | mobike | policy error-notification | rekey | retransmission-timeout | setup-timer } | keepalive | nai | natt }

---

authentication gateway

Configures the default pre-shared gateway key used for authentication.

---

certificate

Configures the system to remove the certificate for a given crypto template.

---

dns-handling

Configures the system to use normal DNS handling.

---

dos cookie-challenge detect-dos-attack

Configures the system to disable any Denial of Service attacks.

---

ikev2-ikesa { ignore-rekeying-requests | keepalive | max-retransmission | mobike | policy error-notification | rekey | retransmission-timeout | setup-timer }

Configures the system to use the following ikev2-ikesa defaults:

- **ignore-rekeying-requests**: Ignore any IKE_SA rekeying requests received.
- **keepalive-user-activity**: Keepalive messages received from peer will not reset the user inactivity timer.
- **max-retransmission**: Set the number of IKEv2 IKE exchange request retransmissions if the corresponding response has not been received. Default is 5.
- **mobike:** Set MOBIKE to disable.
- **policy error-notification**: Set the default policy error notification method to send error notify messages to the MS.
- **rekey**: Set the default rekeying of IKE_SA to disabled.
- **retransmission-timeout**: Set the maximum number of milliseconds to elapse before an IKEv2 IKE exchange request is retransmitted if the corresponding IKEv2 IKE exchange response has not been received to 500.

- **setup timer**: Set the number of seconds to elapse before a non-fully-established IKEv2 IKE SA is terminated to 60.

keepalive

Enables Dead Peer Detection for all SAs derived from this crypto template.

nai

Sets the default NAI parameters to be used for the crypto template (IDr) to none

natt

Enables NAT-T initiation for all SAs derived from this crypto template.

Usage

Use these commands to restore default parameters.

Example

Use the following command to disable MOBIKE by default:

```
default mobike
```

dns-handling

Adds a custom option to define the ways a DNS address is returned based on proscribed circumstances described below.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

```
[ default ] dns-handling { normal | custom }
```

default

Configures the default condition as **normal**. By default, PDIF always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

dns-handling normal

This is the default action. PDIF always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

dns-handling custom

Configures the PDIF to behave as described in the Usage section below.

Usage

During IKEv2 session setup, MS may or may not include INTERNAL_IP4_DNS in the Config Payload (CP). PDIF may obtain one or more DNS addresses for the subscriber in DNS NVSE from a proxy-MIP Registration Reply message. If Multiple Authentication is used, these DNS addresses may be also received in Diameter AVPs during the first authentication phase, or in RADIUS attributes in the Access Accept messages during the second authentication phase.
In **normal** mode, by default PDIF always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.
In **custom** mode, depending on the number of INTERNAL_IP4_DNS, PDIF supports the following behaviors:

- If MS includes no INTERNAL_IP4_DNS in Config Payload: PDIF doesn't return any INTERNAL_IP4_DNS option to MS, whether or not PDIF has received one(s) in DNS NVSE from HA or from local configurations.
- If MS requests one or more INTERNAL_IP4_DNS(s) in Config Payload, and if P-MIP NVSE doesn't contain any DNS address or DNS address not present in any config, PDIF omits INTERNAL_IP4_DNS option to MS in the Config Payload.
- And if P-MIP NVSE includes one DNS address (a.a.a.a / 0.0.0.0), then PDIF sends one INTERNAL_IP4_DNS option in Config Payload back to the MS.
- If the Primary DNS is a.a.a.a and the Secondary DNS is 0.0.0.0, then a.a.a.a is returned (only one instance of DNS attribute present in the config payload).
- If the Primary DNS is 0.0.0.0 and the Secondary DNS is a.a.a.a, then a.a.a.a is returned (only one instance of DNS attribute present in the config payload). PDIF does not take 0.0.0.0 as a valid DNS address that can be assigned to the MS.

- And if P-MIP NVSE includes two DNS addresses (a.a.a.a and b.b.b.b) or configurations exists for these two addresses, then PDIF sends two INTERNAL_IP4_DNSs in the CP for the MS (typically known as primary and secondary DNS addresses).

Example

The following configuration applies the **custom** dns-handling mode:

```
dns-handling custom
```

dos cookie-challenge notify-payload

Configure the cookie challenge parameters for IKEv2 INFO Exchange notify payloads for the given crypto template.

Product

All

Privilege

Administrator

Syntax

```
dos cookie-challenge notify-payload [ half-open-sess-count { start integer | stop integer } ]

[ default | no ] cookie-challenge detect-dos-attack
```

default

Default is to disabled condition.

no

Prevents Denial of Service cookie transmission. This is the default condition.

half-open-sess-count *start* **|** *stop*

The **half-open-sess-count** is the number of half-open sessions per IPSec manager.
A session is considered half-open if a PDIF has responded to an IKEv2 INIT Request with an IKEv2 INIT Response, but no further message was received on that particular IKE SA.

- *start*: Starts when the current half-open-sess-count exceeds the start count. The start count is an integer from 0 to 100000.
- *stop*: Stops when the current half-open-sess-count drops below the stop count. The stop count number is an integer from 0 to 100000. It is always less than or equal to the start count number

Important: The start count value 0 is a special case whereby this feature is always enabled. In this event, both **Start** and **Stop** must be 0.

Usage

This feature (which is disabled by default) helps prevent malicious Denial of Service attacks against the server by sending a challenge cookie. If the response from the sender does not incorporate the expected cookie data, the packets are dropped.

Example

The following example configures the cookie challenge to begin when the half-open-sess-count reaches *50000* and stops when it drops below *20000*:

```
dos cookie-challenge notify-payload half-open-sess-count start 50000 stop 20000
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

ikev2-ikesa

Configures parameters for the IKEv2 IKE Security Associations within this crypto template.

Product

All

Privilege

Administrator

Syntax

ikev2-ikesa { allow-empty-ikesa | keepalive-user-activity | max-retransmissions *number* **| retransmission-timeout** *msec* **| policy error-notification [invalid-message-id | invalid-syntax] rekey | setup-timer** *sec* **| transform-set list** *name* **}**

default ikev2-ikesa { allow-empty-ikesa | max-retransmissions | policy error-notification [invalid-message-id | invalid-syntax] rekey | retransmission-timeout | setup-timer }

no ikev2-ikesa { allow-empty-ikesa | keepalive-user-activity | list *name* **| policy error-notification [invalid-message-id | invalid-syntax] | rekey }**

no ikev2-ikesa

Disables a previously enabled parameter.

allow-empty-ikesa

Default is not to allow-empty-ikesa. Activate to have the IKEv2 stack keep the IKE SA when all the Child SAs have been deleted.

keepalive-user-activity

Default is no keepalive-user-activity. Activate to reset the user inactivity timer when keepalive messages are received from peer.

max-retransmissions *number*

Specifies the maximum number of retransmissions of an IKEv2 IKE exchange request if a response has not been received. *number* must be an integer from 1 through 8. Default: 5

policy error-notification

Default policy is to generate an IKEv2 Invalid Message ID error when PDIF receives an out-of-sequence packet. Default is to enable.

retransmission-timeout *msec*

Specifies the timeout period in milliseconds before a retransmission of an IKEv2 IKE exchange request is sent (if the corresponding response has not been received). *msec* must be an integer from 300 to 15000. Default: 500

rekey

Specifies if IKESA rekeying should occur before the configured lifetime expires (at approximately 90% of the lifetime interval). Default is not to re-key.

setup-timer *sec*

Specifies the number of seconds before a IKEv2 IKE Security Association that is not fully established is terminated. *sec* must be an integer from 1 through 3600. Default: 16

transform-set list *name*

Specifies the name of context-level configured IKEv2 IKE Security Association transform set. *name* must be an existing IKEv2 IKESA Transform Set expressed as an alphanumeric string of 1 through 127 characters.

list

A space-separated list of IKEv2-IKESA SA transform sets to be used for deriving IKEv2 IKE Security Associations from this crypto template. A minimum of one transform-set is required; maximum configurable is six.

Usage

Use this command to configure parameters for the IKEv2 IKE Security Associations within this crypto template.

Example

The following command configures the maximum number of IKEv2 IKESA request retransmissions to *7*:

```
ikev2-ikesa max-retransmissions 7
```

The following command configures the IKEv2 IKESA request retransmission timeout to *400*:

```
ikev2-ikesa retransmission-timeout 400
```

The following command configures the IKEv2 IKESA transform set list name to *ikesa43*:

```
ikev2-ikesa transform-set list ikesa43
```

keepalive

Configures keepalive or dead peer detection for security associations used within this crypto template.

Product

All

Privilege

Security Administrator, Administrator

Syntax

keepalive [interval *sec* **] [timeout** *sec* **] [num-retry** *num* **]**

default keepalive [interval] [timeout] [num-retry]

no keepalive

no

Disables keepalive messaging.

interval *sec*

Specifies the amount of time (in seconds) that must elapse before the next keepalive request is sent. *sec* must be an integer from 10 through 3600. Default: 10

timeout *sec*

Specifies the amount of time (in seconds) that the system will wait without receiving a reply before retrying the keepalive request. *sec* must be an integer from 10 through 3600. Default: 10

num-retry *num*

Specifies the number of times the system will retry a non-responsive peer before defining the peer as off-line or out-of-service. *num* must be an integer from 1 through 100. Default: 2

Usage

Use this command to set parameters associated with determining the availability of peer servers.

Example

The following command sets a keepalive interval to three minutes (*180* seconds), the timeout to *30* seconds, and the retry attempts number to *5*:

```
keepalive interval 180 timeout 30 num-retry 5
```

max-childsa

Defines a soft limit for the number of Child SAs Child SAs per IKEv2 policy.

Product

FNG

Privilege

Security Administrator, Administrator

Syntax

```
max-childsa <1 . . 4> [ overload action < ignore | terminate > ]
```

max-childsa < 1 . . 4 >

Specifies a soft limit for the maximum number of Child SAs per IKEv2 policy, which can be from 1 to 4.

overload-action

The action taken when the specified soft limit for the maximum number of Child SAs is reached, as follows:

- **ignore**: The IKEv2 stack ignores the specified soft limit for Child SAs.
- **terminate**: The IKEv2 stack rejects any new Child SAs if the specified soft limit is reached.

Usage

The FNG maintains two maximum Child SA values per IKEv2 policy. The first is a system-enforced maximum value, which is four Child SAs per IKEv2 policy. The second is a configurable soft maximum value, which can be a value between one and four. This command defines the soft limit for the maximum number of Child SAs per IKEv2 policy.

Example

The following command specifies a soft limit of 2 Child SAs with the overload action of terminate.

```
max-childsa 2 overload action terminate
```

nai

Configures the Network Access Identifier (NAI) parameters to be used for the crypto template IDr.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

[default | no] nai idr *name* **id-type {rfc822-addr | fqdn | ip-addr | key-id }**

default

Configures the default command **no nai idr**. As a result, the default behavior is for the PDIF-service IP address to be sent as the IDr value of type ID_IP_ADDR.

no

no nai idr configures the value whereby the PDIF service IP address is sent as the IDr value with the type ID_IP_ADDR. This is the default condition.

nai idr *name*

Specifies the name of the IDr crypto template as an alphanumeric string of 1 through 79 characters.

id-type { rfc822-addr | fqdn | ip-addr | key-id }

Configures the NAI IDr type parameter. If no id-type is specified, then **rfc822-addr** is assumed.

- **rfc822-addr**: configures NAI Type ID_RFC822_ADDR.
- **fqdn**: configures NAI Type ID_FQDN.
- **ip-addr**: configures NAI Type ID_IP_ADDR.
- **key-id**: configures NAI Type ID_KEY_ID.

Usage

The configured IDr is sent from the PDIF to the MS in the first IKEv2 AUTH response.

Example

The following command configures the NAI IDr to the default condition.

```
no naiidr
```

natt

Configures Network Address Translation - Traversal (NAT-T) for all security associations associated with this crypto template. This feature is disabled by default.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] natt [ send-keepalive ]
```

default

Disables NAT-T for all security associations associated with this crypto template.

no

Disables NAT-T for all security associations associated with this crypto template.

send-keepalive

Sends NAT-Traversal keepalive messages.

Usage

Use this command to configure NAT-T for security associations within this crypto template.

Example

The following command disables NAT-T for this crypto template:

```
no natt
```

payload

Creates a new, or specifies an existing, crypto template payload and enters the Crypto Template Payload Configuration Mode.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

`[ no ] payload` *`name`* **`match childsa [ match { ipv4 | ipv6 } ]`**

`no`

Removes a currently configured crypto template payload.

`payload` *`name`*

Specifies the name of a new or existing crypto template payload as an alphanumeric string of 1 through 127 characters.

`match childsa [ match { ipv4 | ipv6 }`

Filters IPSec Child Security Association creation requests for subscriber calls using this payload. Further filtering can be performed by applying the following:

- **`match ipv4`**: Configures this payload to be applicable to IPSec Child Security Association requests for IPv4.
- **`match ipv6`**: Configures this payload to be applicable to IPSec Child Security Association requests for IPv6.

Usage

Use this command to create a new or enter an existing crypto template payload. The payload mechanism is a means of associating parameters for the Security Association (SA) being negotiated.
Two payloads are required: one each for MIP and IKEv2. The first payload is used for establishing the initial Child SA Tunnel Inner Address (TIA) which will be torn down. The second payload is used for establishing the remaining Child SAs. Note that if there is no second payload defined with home-address as the *`ip-address-allocation`* then no MIP call can be established, just a Simple IP call.
Currently, the only available match is for ChildSA, although other matches are planned for future releases. Omitting the second match parameter for either IPv4 or IPv6 will make the payload applicable to all IP address pools.
Crypto Template Payload Configuration Mode commands are defined in the *Crypto Template IKEv2-Dynamic Payload Configuration Mode Commands* chapter.

Example

The following command configures a crypto template payload called *`payload5`* and enters the Crypto Template Payload Configuration Mode:

```
payload payload5 match childsa
```

peer network

Configures a list of allowed peer addresses on this crypto template.

Product

All

Privilege

Administrator

Syntax

peer network *ip_address* **{/***mask* **| mask** *ip_mask* **} [encrypted pre-shared-key** *key* **| pre-shared-key** *key* **]**

no peer network *ip_address* **mask** *ip_mask*

no

Removes the specified peer network IP address from this crypto template.

peer network *ip_address* **{/***mask* **| mask** *ip_mask* **}**

Specifies the IP address of the peer network in IPv4 dotted-decimal or IPv6 colon-separated notation.
/*mask* specifies the subnet mask bits. *mask* must be and integer value from 1 to 32 for IPv4 addresses and 1 to 128 for IPv6 addresses (CIDR notation).
mask *ip_mask* specifies the subnet mask in IPv4 dotted-decimal or IPv6 colon-separated notations.

[encrypted pre-shared-key *key* **| pre-shared-key** *key* **]**

encrypted preshared key *key*: Specifies that an encrypted pre-shared key is to be used for IPSec authentication for the address range. *key* must be an alphanumeric string or hexadecimal sequence from 16 to 64.
preshared key *key*: Specifies that a pre-shared key is to be used for IPSec authentication for the address range. *key* must be an alphanumeric string or hexadecimal sequence from 1 to 32.

Usage

Use this command to configure a list or range of allowed peer network IP addresses for this template.

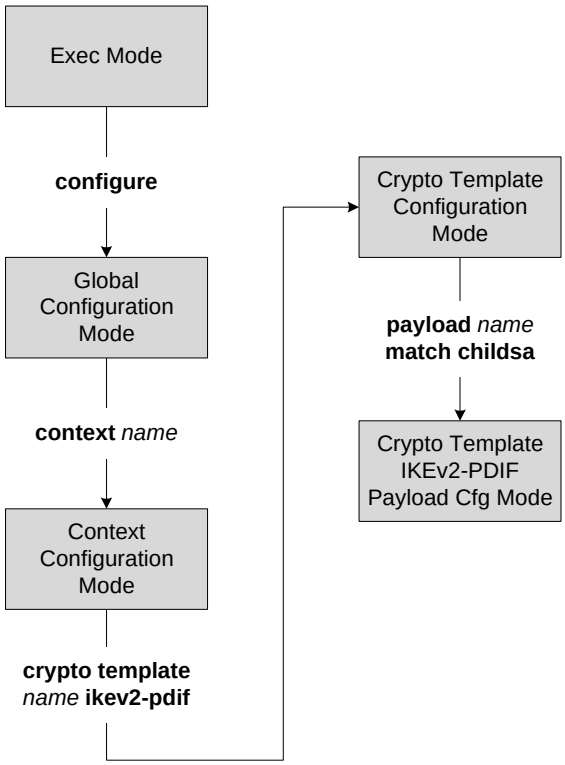
Example

The following command configures a set of IP addresses with starting address of *10.2.3.4* and a bit mask of *8*:

```
peer network 10.2.3.4/8
```

Chapter 63
Crypto Template IKEv2-Dynamic Payload Configuration Mode Commands

The Crypto Template IKEv2-Dynamic Payload Configuration Mode is used to assign the correct IPSec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses. There should be two payloads configured. The first must have a dynamic addressing scheme from which the ChildSA gets a TIA address. The second payload supplies the ChildSA with a HoA, which is the default setting for `ip-address-allocation`.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

default

Sets or restores the default value for the specified parameter.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

```
default { ignore-rekeying-requests | ip-address-allocation lifetime | maximum-child-sa |
rekey | tsi | tsr }
```

ignore-rekeying-requests

Configures the system to ignore IPSec SA rekey requests.

ip-address-allocation

Configures the crypto map payload IP address allocation scheme to be the home address.

lifetime

Configures the default lifetime for IPSec Child SAs derived from this crypto template. **lifetime:** 86400 seconds.

maximum-child-sa

Configures the maximum number of IPSec Child SAs to be derived from an IKEv2 IKE SA by default.

rekey

Configures the system to disable Child SA rekeying.

tsi

Configures the default TSi payload to be that of the mobile endpoint.

tsr

Configures the default TSr payload option.

Usage

Configures system defaults.

Example

Use the following configuration to set the TSi payload start-address to be that of the mobile endpoint:

```
default tsi
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

ignore-rekeying-requests

Ignores CHILD SA rekey requests from the Packet Data Interworking Function (PDIF).

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

```
ignore-rekeying-requests
```

Usage

Prevents creation of a CHILD SA based on this crypto template.

Example

The following command prevents creation of a CHILD SA based on this crypto template:

```
ignore-rekeying-requests
```

ip-address-allocation

Configures IP address allocation for subscribers using this crypto template payload. Configure two payloads per crypto template. The first must have a dynamic address to assign a tunnel inner address (TIA) to the ChildSA. The second payload is configured after a successful MAnaged IP (MIP) initiation and can use the default Home Address (HoA) option.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

```
ip-address-allocation { dynamic | home-address | static }

default ip-address-allocation
```

ip-address-allocation dynamic

Specifies that the IP address for the subscriber is allocated from a dynamic IP pool.

ip-address-allocation home-address

The IP address for the subscriber is allocated by the Home Agent. This is the default setting for this command.

ip-address-allocation static

The IP address for the subscriber is a static simple IP address.

Usage

Use this command to configure how ChildSA payloads are allocated IP addresses for this crypto template.

Example

The following command is for the first ChildSA and will ensure that it gets a TIA address from an IP address pool:

```
ip-address-allocation dynamic
```

The following command is for the second ChildSA and will ensure that it gets a HoA address from the HA:

```
default ip-address-allocation
```

ipsec

Configures the IPSec transform set to be used for this crypto template payload.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

[no] ipsec transform-set list *name*

no

Specifies the IPSec transform set to be deleted. This is a space-separated list. From 1 to 4 transform sets can be entered. *name* must be an alphanumeric string of 1 through 127 characters.

ipsec transform-set list *name*

Specifies the context configured IPSec transform set name to be used in the crypto template payload. This is a space-separated list. From 1 to 4 transform sets can be entered. *name* must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to list the IPSec transform set(s) to use in this crypto template payload.

Example

The following command configures IPSec transform sets named *ipset1* and *ipset2* to be used in this crypto template payload:

```
ipsec transform-set list ipset1 ipset2
```

lifetime

Configures the number of seconds for IPSec Child SAs derived from this crypto template payload to exist.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

lifetime *sec*

default lifetime

lifetime *sec*

Specifies the number of seconds for IPSec Child Security Associations derived from this crypto template payload to exist. *sec* is an integer from 60 through 86400. Default: 86400

default lifetime

Sets the lifetime to its default value of 86400 seconds.

Usage

Use this command to configure the number of seconds for IPSec Child Security Associations derived from this crypto template payload to exist.

Example

The following command configures the IPSec child SA lifetime to be *120* seconds:

```
lifetime 120
```

maximum-child-sa

Configures the maximum number of IPSec child security associations that can be derived from a single IKEv2 IKE security association.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

maximum-child-sa *num*

default maximum-child-sa

maximum-child-sa *num*

Specifies the maximum number of IPSec child security associations that can be derived from a single IKEv2 IKE security association. *num* must be 1. Default: 1

default maximum-child-sa

Sets the maximum number of Child SAs to its default value of 1.

Usage

Use this command to configure the maximum number of IPSec child security associations that can be derived from a single IKEv2 IKE security association.

Example

The following command configures the maximum number of child SAs to 1:

```
maximum-child-sa 1
```

rekey

Configures IPSec Child Security Association rekeying.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] rekey [ keepalive ]
```

no

Disables this feature.

keepalive

If specified, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default, rekeying is only performed if there has been data exchanged since the previous rekey.

Usage

Use this command to enable or disable the ability to rekey IPSec Child SAs after approximately 90% of the Child SA lifetime has expired. The default, and recommended setting, is not to perform rekeying. No rekeying means the PDIF will not originate rekeying operations and will not process CHILD SA rekeying requests from the UE.

Example

The following command disables rekeying:

```
no rekey
```

tsi

Configures the IKEv2 Traffic Selector-Initiator (TSi) payload address options.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

tsi start-address { any { end-address any } | endpoint { end-address *endpoint* **} }**

any { end-address any }

Configures the TSi payload to allow all IP addresses.

endpoint { end-address *endpoint* **}**

Configures the TSi payload start-address to be that of the Mobile endpoint. This is the default value. *endpoint* is the mobile endpoint netmask.

Usage

On receiving a successful IKE_SA_INIT Response from PDIF, the MS sends an IKE_ AUTH Request for the first EAP-AKA authentication. If the MS is capable of doing multiple-authentication, it includes the MULTI_AUTH_SUPPORTED Notify payload in the IKE_AUTH Request. MS also includes an IDi payload containing the NAI, SA, TSi, TSr, and CP (requesting IP address and DNS address) payloads.

Example

Use the following example to configure a TSi payload that allows all addresses:

```
tsi start-address any end-address any
```

tsr

Configures the IKEv2 Traffic Selector-Responder (TSr) payload address options.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

tsr start-address *ipv4 address* **end-address** *ipv4 address*

start-address *ipv4 address*

Configures the TSr payload to include the TSr start IPv4 address of an address range for the Phase 1 multiple traffic selector feature.

end-address *ipv4 address*

Configures the TSr payload start-address to include the IPv4 address of the TSr end of an address range for the Phase 1 multiple traffic selector feature.

Usage

As part of Phase 1 of the Multiple Traffic Selector feature, this command is used to specify an IPv4 address range in the single TSr payload that the PDG/TTG returns in the last IKE_AUTH message. This TSr is Child SA-specific.

Example

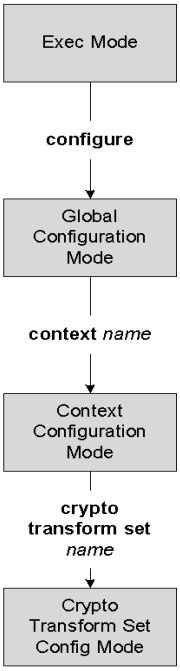
Use the following example to configure a TSr payload that specifies an IPv4 address range for the payload:

```
tsr start-address ipv4 10.2.3.4 end-address 10.2.3.155
```

Chapter 64
Crypto Transform Set Configuration Mode Commands

The Crypto Transform Set Configuration Mode is used to configure properties for system transform sets.

Transform Sets are used to define IPSec security associations (SAs). IPSec SAs specify the IPSec protocols to use to protect packets.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

mode

Configures the IPSec encapsulation mode.

Product

PDSN, HA, GGSN, PDIF

Privilege

Security Administrator, Administrator

Syntax

```
mode { transport | tunnel }
```

mode transport

Specifies that the transform set only protects the upper layer protocol data portions of an IP datagram, leaving the IP header information unprotected. Default: Disabled

Important: This mode should only be used if the communications end-point is also the cryptographic end-point.

mode tunnel

Specifies that the transform set protects the entire IP datagram.
This mode should be used if the communications end-point is different from the cryptographic end-point as in a VPN. Default: Enabled

Usage

This command specifies the encapsulation mode for the transform set.

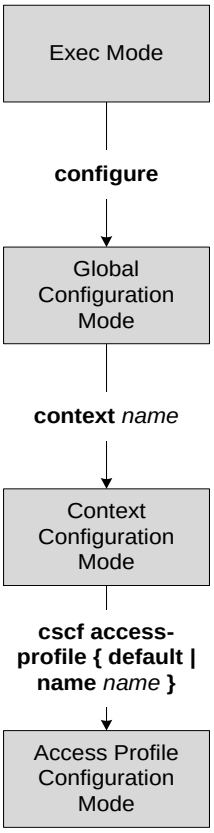
Example

The following command configures the transforms set's encapsulation mode to transport:

```
mode transport
```

Chapter 65
CSCF Access Profile Configuration Mode Commands

The Access Profile Configuration Mode is used to set commands supporting the use of signaling compression, authentication, and SIP timers for subscribers accessing the system from varying network types.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

access-security-type

Sets the type of access security for a P-CSCF/A-BG.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ no ] access-security-type ipsec-3gpp-cscf
```

no

Disables the selected access security type.

ipsec-3gpp-cscf

Security mechanism 3GPP/3GPP2 IPSec.

Usage

Use this command to enable or disable an access security type for a P-CSCF or A-BG.

Example

Enables 3GPP/3GPP2 IPSec access security on P-CSCF or A-BG:

```
access-security-type ipsec-3gpp-cscf
```

Disables 3GPP/3GPP2 IPSec access security on P-CSCF or A-BG:

```
no access-security-type ipsec-3gpp-cscf
```

authentication

Sets the authentication method to use for subscribers using this access profile.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ no ] authentication { aka-v1 | custom-md5 | md5 }
```

no

Disables the selected authentication type.

aka-v1 | custom-md5 | md5

aka-v1: Specifies that the AKA-v1 algorithm will be used for subscribers using this access profile.
custom-md5: Specifies that custom algorithm HTTP-Digest-MD5 will be used for subscribers using this access profile.
md5: Specifies that the MD5 algorithm will be used for subscribers using this access profile. This is the default setting for this command.

Usage

Use this command to set the authentication method used for subscribers using this access profile.

Example

The following command sets the authentication type for subscribers using this access profile to **md5**:

```
authentication md5
```

diameter-selection

Enables or disables prefix and capability-based CDF server selection for this access profile. By default, this command is disabled.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
[ no ] diameter-selection cdf
```

no

Disables prefix and capability-based CDF server selection.

Usage

Use this command to enable or disable prefix and capability-based CDF server selection per access-type.

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

pcrf-policy-control

Enables PCRF policy control for this access profile.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ default | no ] pcrf-policy-control
```

default | no

PCRF policy control is disabled.

Usage

Use this command to enable or disable PCRF policy control for this access profile.

sigcomp

Enables signalling compression for the Access Profile.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ no ] sigcomp [ force ]
```

no

Disables signalling compression for the Access Profile.

force

Specifies that signaling compression is to be forced for the access type. When this feature is enabled, messages received by the P-CSCF/A-BG that are not compressed are rejected.

Usage

Use this command to enable signalling compression for the specific Access Profile.

timeout

Sets timeout values for CSCF and SIP transactions for subscribers using this Access Profile.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
timeout sip { 3gpp-d sec | 3gpp-t1 msec | 3gpp-t2 sec | 3gpp-t4 sec | c sec | d sec |
invite-expiry sec | t1 msec | t2 sec | t4 sec }

default timeout sip { 3gpp-d | 3gpp-t1 | 3gpp-t2 | 3gpp-t4 | c | d | invite-expiry | t1 |
t2 | t4 }
```

---

sip { 3gpp-d *sec* **| 3gpp-t1** *msec* **| 3gpp-t2** *sec* **| 3gpp-t4** *sec* **| c** *sec* **| d** *sec* **| invite-expiry** *sec* **| t1** *msec* **| t2** *sec* **| t4** *sec* **}**

Sets transaction and expiry timers for SIP.
3gpp-d *sec*: This time is used to control the retransmission of 200OK messages to INVITEs after an ACK is sent. The ACK transaction is cleared after this period. This timer is applicable only for unreliable transport.
sec must be an integer from 0 to 2147483646.
Default: 64*T1 (128 seconds, recommended minimum)
3gpp-t1 *msec*: This timer is used to control the time interval between each retransmission. The interval doubles after each retransmission. This is used by P-CSCF/A-BG only when it sending message toward the UE. Example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable transport.
msec must be an integer from 0 to 2147483646.
Default: 2000 ms (2 secs, recommended minimum).
3gpp-t2 *sec*: This timer is used to control the period for which the request continues to get retransmitted. This is used by P-CSCF/A-BG only when it sending message toward the UE. This timer is applicable both for reliable and unreliable transport.
sec must be an integer from 0 to 2147483646.
Default: 16 seconds (recommended minimum).
3gpp-t4 *sec*: This timer is used to control the period for which the final response to non-invite transaction should be buffered. The buffered response for the retransmitted non-invite request should be sent within that interval. This timer is applicable only for unreliable transport.
sec must be an integer from 0 to 2147483646.
Default: 17 seconds (recommended minimum).
c *sec*: This timer is used for an INVITE transaction; if the response is a provisional response with status codes 101 to 199 inclusive (anything but 100), the proxy must reset timer C for that client transaction. The timer may be reset to a different value, but this value must be greater than 3 minutes (180 seconds). When timer C in S-CSCF fires first, S-CSCF will send CANCEL request to Terminating P-CSCF and Terminating P-CSCF will send CANCEL request to UAS .
sec must be an integer from 180 to 2147483646.
Default: 180 seconds
d *sec*: This time is used to control the retransmission of 200 OK to INVITE after ACK is sent. The ACK transaction will be cleared after this interval. This timer is applicable only for unreliable transport.
sec must be an integer from 0 to 2147483646.
Default: 64*T1 (32 seconds, recommended minimum)

invite-expiry *sec*: This timer is used by SIP while acting as UA Role and no final response is received for the INVITE request sent. This timer is applicable for both reliable and unreliable transport.
sec must be an integer from 0 to 2147483646.
Default: 100 seconds (recommended minimum).
t1 *msec*: Specifies the time interval (in milliseconds) between each retransmission. The interval doubles after each retransmission, for example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable transport.
msec must be an integer from 0 to 2147483646.
Default: 500 milliseconds (recommended minimum).
t2 *sec*: This timer is used to control the period for which the request keeps getting retransmitted. This timer is applicable both for reliable and unreliable transport.
sec must be an integer from 0 to 2147483646. The recommended minimum value for this parameter is 4 seconds.
Default: 64*T1 (32 seconds)
t4 *sec*: This timer is used to control the period for which the final response to non-invite transaction should be buffered so as to send the buffered response for the retransmitted non-invite request within that interval. This timer is applicable only for unreliable transport.
sec must be an integer from 0 to 2147483646.
Default: 5 seconds (recommended minimum).

default

Sets/restores default value assigned for specified parameter.

Usage

Use this command to configure SIP Stack timers and CSCF service specific timers for subscriber traffic using this Access Profile.

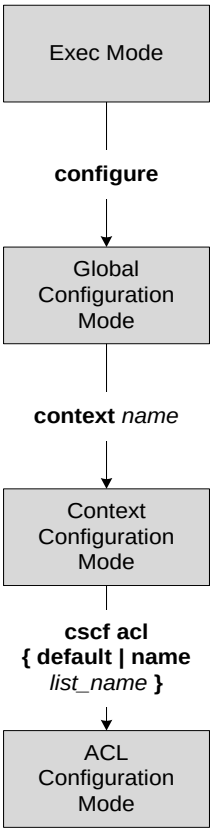
Example

The following command sets the SIP d timer to *64* seconds:

```
timeout sip d 64
```

Chapter 66
CSCF ACL Configuration Mode Commands

The CSCF ACL (Access Control List) Configuration Mode is used to configure session permissions (permit/deny access) within the system.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

after

Places the CSCF ACL entry at the bottom or end of the ACL. Use this command in conjunction with the **permit** and/or **deny** commands.

Product

SCM

Privilege

Administrator

Syntax

after

Usage

Add this command before the **permit** and/or **deny** commands to place the entry at the end of the ACL.

before

Places the CSCF ACL entry at the beginning or top of the ACL. Use this command in conjunction with the **permit** and/or **deny** commands.

Product

SCM

Privilege

Administrator

Syntax

before

Usage

Add this command before the **permit** and/or **deny** commands to place the entry at the beginning of the ACL.

deny

Configures the system to deny subscriber sessions based on criteria matching the received packet.

Product

SCM

Privilege

Administrator

Syntax

deny { any | destination aor *aor* **| log { any | destination aor** *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability** *capability_type* **| user-agent device-type** *device_type* **} | source { address** *ip_address* **| aor** *aor* **} | subscriber-capability** *capability_type* **| user-agent device-type** *device_type* **} +**

no deny { any | destination aor *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability** *capability_type* **}**

any

Filters all CSCF sessions.

destination aor *aor*

Filters sessions based on the destination AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

log { any | destination aor *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability {** *capability_type* **} | user-agent device-type** *device_type* **}**

Enables logging for CSCF sessions meeting the criteria specified in the ACL. The logs can be viewed by executing the **logging filter active facility acl-log** command in the Exec mode.
Specifies the criteria that packets will be compared against. The following criteria are supported:

- **any**
- **destination aor** *aor*
- **source address** *ip_address*
- **source aor** *aor*
- **subscriber-capability** *capability_type*
- **user-agent device-type** *device_type*

source { address *ip_address* **| aor** *aor* **}**

Filters session based on the source IP address or AoR.

- *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
- *aor* must be an existing AoR from 1 to 79 characters in length.

Important: AoR regular expressions are supported. Refer to the *SCM Engineering Rules* Appendix in the *Cisco ASR 5000 Series Session Control Manager Administration Guide* for more information about regular expressions.

subscriber-capability { *capability_type* }

Filters session based on one of the following subscriber capability types:

- **at** - Custom AT Type
- **audio** - Audio Capability Type
- **chat** - Custom CHAT Type
- **cs** - Custom CS Type
- **ft** - Custom FT Type
- **im** - Custom IM Type
- **mms** - Custom MMS Type
- **msg** - Custom MSG Type
- **oma-sip-im** - Custom OMA SIP-IM Type
- **rcs-dp** - Custom RCS-DP Type
- **rcs-e** - Custom RCS-E Type
- **rcs-ft** - Custom RCS-FT Type
- **rcs-im** - Custom RCS-IM Type
- **rcs-is** - Custom RCS-IS Type
- **rcs-sp** - Custom RCS-SP Type
- **rcs-vs** - Custom RCS-VS Type
- **text** - Text Capability Type
- **video** - Video Capability Type
- **vt** - Custom VT Type
- **vt-ft** - Custom VT-FT Type
- **vt-is** - Custom VT -IS Type
- **vt-loc** - Custom VT-LOC Type
- **vt-memo** - Custom VT-MEMO Type

user-agent device-type *device_type*

Filters session based on device-type in user-agent header.
device_type must be from 1 to 15 characters in length. The following user agent device types are supported.

- feature_phone
- smart_phone
- pad
- tablet_pc
- pc

- soft_phone
- modem

+

This symbol indicates that the keywords can be entered multiple times within a single command.

no deny { any | destination aor *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability {** *capability_type* **} }**

Removes specified filter criteria.

Usage

Specifies the subscriber sessions to deny based on the criteria specified.

Example

The following command denies access to subscribers with a source address of *1.2.3.4*:

```
deny source address 1.2.3.4
```

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

```
exit
```

Usage

Return to the previous mode.

permit

Configures the system to allow subscriber sessions based on criteria matching the received packet.

Product

SCM

Privilege

Administrator

Syntax

permit { any | destination aor *aor* **| log { any | destination aor** *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability** *capability_type* **| user-agent device-type** *device_type* **} | source { address** *ip_address* **| aor** *aor* **} | subscriber-capability** *capability_type* **| user-agent device-type** *device_type* **} +**

no permit { any | destination aor *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability** *capability_type* **}**

any

Filters all CSCF sessions.

destination aor *aor*

Filters sessions based on the destination AoR.
aor must be an existing AoR from 1 to 79 characters in length.

Important: AoR regular expressions are supported. Refer to the *SCM Engineering Rules* Appendix in the *Cisco ASR 5000 Series Session Control Manager Administration Guide* for more information about regular expressions.

log { any | destination aor *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability { ***capability_type* **} | user-agent device-type** *device_type* **}**

Enables logging for CSCF sessions meeting the criteria specified in the ACL. The logs can be viewed by executing the **logging filter active facility acl-log** command in the Exec mode.
Specifies the criteria that packets will be compared against. The following criteria are supported:

- **any**
- **destination aor** *aor*
- **source address** *ip_address*
- **source aor** *aor*
- **subscriber-capability** *capability_type*
- **user-agent device-type** *device_type*

source { address *ip_address* **| aor** *aor* **}**

Filters session based on the source IP address or AoR.

- *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
- *aor* must be an existing AoR from 1 to 79 characters in length.

Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

subscriber-capability { *capability_type* **}**

Filters session based on one of the following subscriber capability types:

- **at** - Custom AT Type
- **audio** - Audio Capability Type
- **chat** - Custom CHAT Type
- **cs** - Custom CS Type
- **ft** - Custom FT Type
- **im** - Custom IM Type
- **mms** - Custom MMS Type
- **msg** - Custom MSG Type
- **oma-sip-im** - Custom OMA SIP-IM Type
- **rcs-dp** - Custom RCS-DP Type
- **rcs-e** - Custom RCS-E Type
- **rcs-ft** - Custom RCS-FT Type
- **rcs-im** - Custom RCS-IM Type
- **rcs-is** - Custom RCS-IS Type
- **rcs-sp** - Custom RCS-SP Type
- **rcs-vs** - Custom RCS-VS Type
- **text** - Text Capability Type
- **video** - Video Capability Type
- **vt** - Custom VT Type
- **vt-ft** - Custom VT-FT Type
- **vt-is** - Custom VT -IS Type
- **vt-loc** - Custom VT-LOC Type
- **vt-memo** - Custom VT-MEMO Type

user-agent device-type *device_type*

Filters session based on device-type in user-agent header.
device_type must be from 1 to 15 characters in length. The following user agent device types are supported.

- feature_phone
- smart_phone
- pad
- tablet_pc
- pc

- soft_phone
- modem

+

This symbol indicates that the keywords can be entered multiple times within a single command.

no permit { any | destination aor *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability {** *capability_type* **} }**

Removes specified filter criteria.

Usage

Specifies the subscriber sessions to permit based on the criteria specified.

Example

The following command permits access to subscribers with a destination AoR of *$.@abc123.com*:

```
permit destination aor $.@abc123.com
```

redirect

Configures the system to redirect subscriber sessions to another CSCF based on criteria matching the received packet.

Product

SCM

Privilege

Administrator

Syntax

redirect { address *ip_address* **| host** *host_name* **} [port** *port_number* **] { any | destination aor** *aor* **| log { any | destination aor** *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability** *capability_type* **| user-agent device-type** *device_type* **} | source { address** *ip_address* **| aor** *aor* **} | subscriber-capability** *capability_type* **| user-agent device-type** *device_type* **} +**

no redirect { address *ip_address* **| host** *host_name* **} [port** *port_number* **] { any | destination aor** *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability** *capability_type* **}**

address *ip_address*

The address to which UE should be redirected.
ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

host *host_name*

The host to which UE should be redirected.
host_name must be an existing name from 1 to 79 characters in length.

port *port_number*

The port at which request should be redirected.
port_number must be an integer from 1 to 65535.

any

Redirect UE to address/host.

destination aor *aor*

Redirect UE to address/host if destination AoR matches.
aor must be an existing AoR from 1 to 79 characters in length.

Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

log { any | destination aor *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability { ** *capability_type* **} | user-agent device-type** *device_type* **}**

Enables logging for redirect ed UE meeting the criteria specified in the ACL. The logs can be viewed by executing the **logging filter active facility acl-log** command in the Exec mode.

Specifies the criteria that packets will be compared against. The following criteria are supported:

- **any**
- **destination aor** *aor*
- **source address** *ip_address*
- **source aor** *aor*
- **subscriber-capability** *capability_type*
- **user-agent device-type** *device_type*

---

source { address *ip_address* **| aor** *aor* **}**

Redirect UE to address/host if source IP address or AoR matches.

- *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
- *aor* must be an existing AoR from 1 to 79 characters in length.

Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

---

subscriber-capability { *capability_type* **}**

Redirect UE to address/host if contact has one of the following subscriber capability types:

- **at** - custom AT type
- **audio** - audio capability type
- **chat** - custom CHAT type
- **cs** - custom CS type
- **ft** - custom FT type
- **im** - custom IM type
- **mms** - custom MMS type
- **msg** - Custom MSG Type
- **oma-sip-im** - Custom OMA SIP-IM Type
- **rcs-dp** - Custom RCS-DP Type
- **rcs-e** - Custom RCS-E Type
- **rcs-ft** - Custom RCS-FT Type
- **rcs-im** - Custom RCS-IM Type
- **rcs-is** - Custom RCS-IS Type
- **rcs-sp** - Custom RCS-SP Type
- **rcs-vs** - Custom RCS-VS Type
- **text** - Text Capability Type
- **video** - Video Capability Type
- **vt** - Custom VT Type
- **vt-ft** - Custom VT-FT Type
- **vt-is** - Custom VT -IS Type

- **vt-loc** - Custom VT-LOC Type
- **vt-memo** - Custom VT-MEMO Type

---

user-agent device-type *device_type*

Redirect UE to address/host according to device-type in user-agent header.
device_type must be from 1 to 15 characters in length. The following user agent device types are supported.

- feature_phone
- smart_phone
- pad
- tablet_pc
- pc
- soft_phone
- modem

+

This symbol indicates that the keywords can be entered multiple times within a single command.

---

no redirect { address *ip_address* **| host** *host_name* **} [port** *port_number* **] { any | destination aor** *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability {** *capability_type* **} }**

Removes specified redirect location and filter criteria.

Usage

Specifies the subscriber sessions to redirect based on the criteria specified.

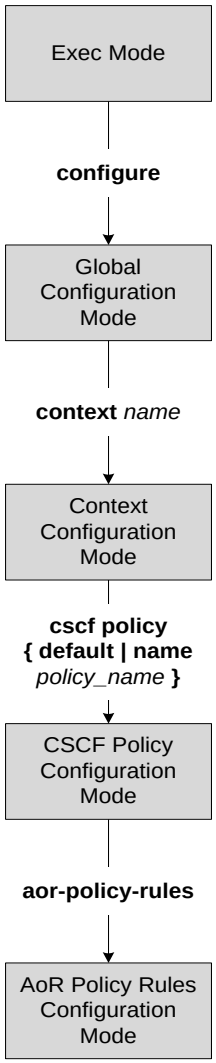
Example

The following command redirects subscribers with a destination AoR of *$.@abc123.com* to host *scscf.com*:

```
redirect host scscf.com destination aor $.@abc123.com
```

Chapter 67
CSCF AoR Policy Rules Configuration Mode Commands

The CSCF AoR Policy Rules Configuration Mode is used to manage AoR policy profiles within the system. Both default and user-defined profiles can be managed in this mode.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

after

Places the CSCF policy entry at the bottom or end of the policy list. Use this command in conjunction with the **aor** command.

Product

SCM

Privilege

Administrator

Syntax

after

Usage

Add this command before the **aor** command to place the entry at the end of the policy list.

aor

Configures an AoR profile and enters the AoR Profile Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

[no] aor *aor_name*

no

Removes the AoR profile from the system.

aor_name

Specifies a name for the AoR profile.
aor_name must be from 1 to 79 alpha and/or numeric characters in length.

Usage

Use this command to create or modify an AoR profile and enter the CSCF Policy Rules Configuration Mode. Entering this command results in the following prompt:
[*context_name*]*hostname*(config-*aor_name*-aor)#
CSCF Policy Rules Configuration Mode commands are defined in the CSCFPolicy Rules Configuration Mode Commands chapter of this guide.

Example

The following command creates an AoR profile named *aor5* and enters the AoR Profile Configuration Mode:

```
aor aor5
```

before

Places the CSCF policy entry at the top or beginning of the policy list. Use this command in conjunction with the **aor** command.

Product

SCM

Privilege

Administrator

Syntax

before

Usage

Add this command before the **aor** command to place the entry at the beginning of the policy list.

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

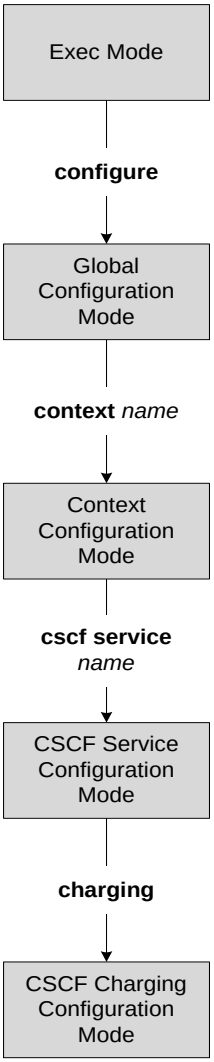
```
exit
```

Usage

Return to the previous mode.

Chapter 68
CSCF Charging Configuration Mode Commands

The CSCF Charging Configuration Mode is used to manage CSCF service policy profiles within the system.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exclude

Configures the service to exclude SIP requests from the Rf charging configuration.

Product

SCM

Privilege

Administrator

Syntax

[no] exclude { custom *sip_method* **| invite | message | notify | register | subscribe | update }**

no

Removes the exclusion of the specified SIP request message type.

custom *sip_method*

Specifies CUSTOM SIP requests that are to be excluded from Rf charging.
sip_method can be a name of any SIP method and be from 1 to 31 alpha and/or numeric characters.

invite

Specifies that INVITE SIP requests are to be excluded from Rf charging.

message

Specifies that MESSAGE SIP requests are to be excluded from Rf charging.

notify

Specifies that NOTIFY SIP requests are to be excluded from Rf charging.

register

Specifies that REGISTER SIP requests are to be excluded from Rf charging.

subscribe

Specifies that SUBSCRIBE SIP requests are to be excluded from Rf charging.

update

Specifies that UPDATE SIP requests are to be excluded from Rf charging.

Usage

Use this command to exclude specific SIP requests from Rf charging.

Example

The following command configures the service to exclude SIP REGISTER requests from Rf charging:

```
exclude register
```

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

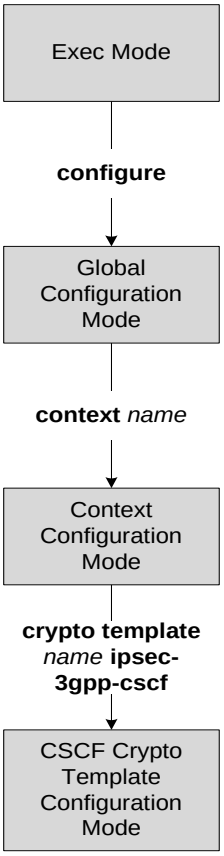
```
exit
```

Usage

Return to the previous mode.

Chapter 69
CSCF Crypto Template Configuration Mode Commands

The CSCF Crypto Template Configuration Mode is used to configure a P-CSCF IPsec policy. It includes most of the IPsec parameters and Internet Key Exchange version 1 (IKEv1) parameters for cryptographic and authentication algorithms etc. A P-CSCF service will not support IPSec without a configured crypto template. Only one crypto template can be configured per P-CSCF service.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec Mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Returns to the previous mode.

ipsec

Configures parameters for the 3GPP/3GPP2 P-CSCF security associations within this crypto template.

Product

SCM

Privilege

Security Administrator, Administrator

Syntax

ipsec transform-set list *list_name*

transform-set list *name*

transform-set: Specifies a context-level IPSec security association transform set to be used for deriving 3GPP/3GPP2 P-CSCF security associations from this crypto template.
list *list_name:* A space separated list of 3GPP/3GPP2 P-CSCF security association transform sets. *list_name* must be an existing 3GPP/3GPP2 P-CSCF transform set and be from 1 to 127 alpha and/or numeric characters.

Important: A minimum of one transform set is required. A maximum of four transform sets may be specified.

Usage

Use this command to configure parameters for the 3GPP/3GPP2 P-CSCF security associations within this crypto template.

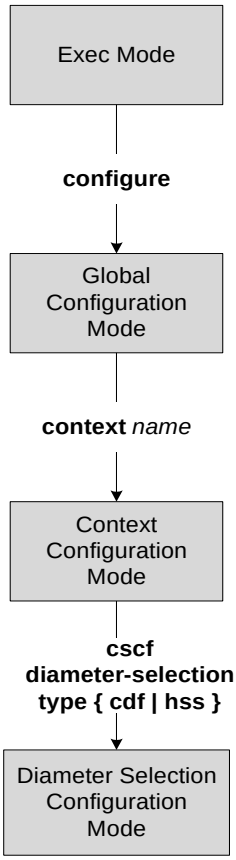
Example

The following command configures the 3GPP/3GPP2 P-CSCF transform set list name to *ikev1list1*:

```
ipsec transform-set list ikev1list1
```

Chapter 70
CSCF Diameter Selection Configuration Mode Commands

The Diameter Selection Configuration Mode is used to configure AAA group selection criteria that will be used for all CDF (enabled for a given access type) or HSS interactions for a subscriber.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

aaa-group

Configures diameter selection entries.

Product

SCM

Privilege

Administrator

Syntax

aaa-group *name* **{ [preference** *value* **] criteria { aor** *aor_prefix* **| subscriber-capability** *capability_type* **| subscriber-ip-type { v4 | v6 } } +**

no aaa-group *name* **preference** *value*

name

Specifies a name for the diameter selection entry.
name must be from 1 to 63 alpha and/or numeric characters.

preference *value*

Configures preference that will be associated with each diameter selection entry. If preference is specified, the entry matching the preference is updated and a new entry is created in the prefix table. If preference is not specified, it is assigned a preference one greater than the last entry's preference in the diameter selection table.
value must be an integer from 1 to 65535.

criteria

Specifies AAA group selection criteria.

aor *aor_prefix*

Filters based on the source or destination AoR.
aor_prefix must be an existing AoR from 1 to 79 characters in length.

Important: AoR regular expressions are supported. Refer to the *SCM Engineering Rules* Appendix in the *Cisco ASR 5000 Series Session Control Manager Administration Guide* for more information about regular expressions.

subscriber-capability *capability_type*

Filters based on the capability of the subscriber.

- **at** - Custom AT Type
- **audio** - Audio Capability Type
- **chat** - Custom CHAT Type
- **cs** - Custom CS Type
- **ft** - Custom FT Type
- **im** - Custom IM Type

- **mms** - Custom MMS Type
- **msg** - Custom MSG Type
- **oma-sip-im** - Custom OMA SIP-IM Type
- **rcs-dp** - Custom RCS-DP Type
- **rcs-e** - Custom RCS-E Type
- **rcs-ft** - Custom RCS-FT Type
- **rcs-im** - Custom RCS-IM Type
- **rcs-is** - Custom RCS-IS Type
- **rcs-sp** - Custom RCS-SP Type
- **rcs-vs** - Custom RCS-VS Type
- **text** - Text Capability Type
- **video** - Video Capability Type
- **vt** - Custom VT Type
- **vt-ft** - Custom VT-FT Type
- **vt-is** - Custom VT -IS Type
- **vt-loc** - Custom VT-LOC Type
- **vt-memo** - Custom VT-MEMO Type

---

subscriber-ip-type { v4 | v6 }

Filters based on the IP type of the subscriber.
v4 - IPv4 type
v6 - IPv6 type

+

This symbol indicates that the keywords can be entered multiple times within a single command.

---

no aaa-group *name* **preference** *value*

Removes configured diameter selection entry.

Usage

This command configures matching criteria for selecting a AAA group name. When a subscriber registers, the selection criteria are compared and the AAA group name from the matching entry will be picked up. The selected aaa-group will be used for all CDF (enabled for a given access type) or HSS interactions for that subscriber.

Example

The following command creates a diameter selection entry named *aaa1*, with a destination AoR criteria of *$.@abc123.com* and preference 125 associated with it:

```
aaa-group aaa1 preference 125 criteria aor $.@abc123.com
```

The following command (immediately following in the configuration file) creates a diameter selection entry named *aaa2*, with a destination AoR criteria of *user@cisco.com* and preference 126 automatically associated with it:

```
aaa-group aaa2 criteria aor user@cisco.com
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

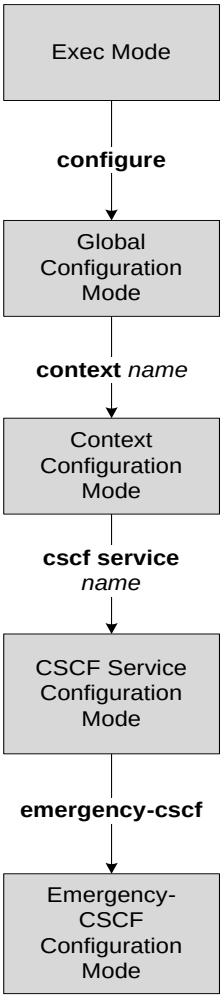
```
exit
```

Usage

Use this command to return to the parent configuration mode.

Chapter 71
CSCF Emergency-CSCF Configuration Mode Commands

The Emergency-CSCF Configuration Mode is used to set commands supporting the role of the CSCF service as an Emergency CSCF.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

exit

Usage

Return to the previous mode.

privacy

Enables privacy support on the E-CSCF.

Product

SCM

Privilege

Administrator

Syntax

```
[ no | default ] privacy
```

no | default

Removes privacy support from the E-CSCF.

Usage

Use this command to enable privacy support for Emergency CSCF service.

psap-file

Sets the location of the PSAP-Database file to maintain and access the ESRK-Ranges provided by the operator for the E-CSCF.

Product

SCM

Privilege

Administrator

Syntax

psap-file *file_name*

no psap-file

no

Removes the PSAP-Database file from the E-CSCF.

file_name

Specifies the PSAP-Database file in one of the following formats:

- ftp://[username]:[password]@host[/directory]/<filename>
- file:/flash[/directory]/<filename> - URL

Usage

This command is used by the SRDB proclet for ESRK-PSAP database management for the E-CSCF.

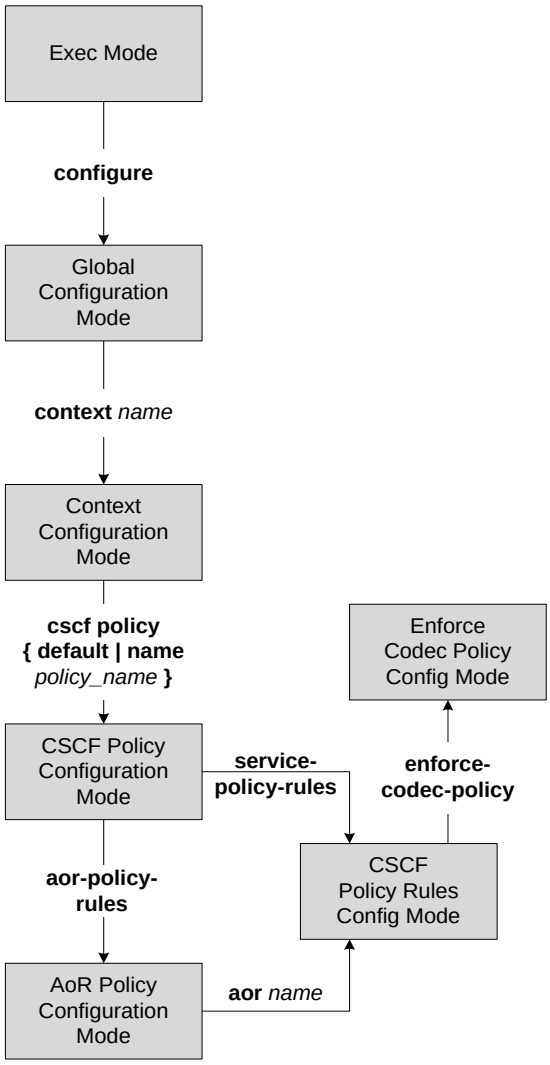
Example

The following command specifies a PSAP-Database file for the E-CSCF:

```
psap-file
ftp://[username]:[password]@10.6.2.246/home/nthattil/psap_profile_CSV_new1.csv
```

Chapter 72
CSCF Enforce Codec Policy Configuration Mode Commands

The CSCF Enforce Codec Policy Configuration Mode is used to manage audio and video codec policies within the system. The parameters defined in this chapter are derived from IETF RFC 3551: “RTP Profile for Audio and Video Conferences with Minimal Control”.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

dynamic-codec

Creates a list of dynamic codecs supported by the system.

Product

SCM

Privilege

Administrator

Syntax

dynamic-codec { audio *encoding_name* **| video** *encoding_name* **} [** *clock_rate* **] [** *channels* **]**

default dynamic-codec

no dynamic-codec [*encoding_name* **] [** *clock_rate* **] [** *channels* **]**

---

audio *encoding_name* **| video** *encoding_name*

audio *encoding_name:* Specifies the encoding name of the dynamic audio codec added to the allowed codec list. *encoding_name* must be from 1 to 49 alpha and/or numeric characters.
video *encoding_name:* Specifies the encoding name of the dynamic video or audio-video codec added to the allowed codec list. *encoding_name* must be from 1 to 49 alpha and/or numeric characters.

[*clock_rate* **] [** *channels* **]**

clock_rate: Specifies the sampling rate of the codec. *clock_rate* must be an integer from 0 to 1000000.
channels: Specifies the number of channels required by the codec. *channels* must be an integer from 1 to 1000000.
Valid dynamic audio codecs:

Encoding Name	Clock Rate (Hz)	Channels
G726-40	8,000	1
G726-32	8,000	1
G726-24	8,000	1
G726-16	8,000	1
G729D	8,000	1
G729E	8,000	1
GSM-EFR	8,000	1
L8	Variable	Variable
RED	See RFC3551	
VDVI	Variable	1

Valid dynamic video codecs:

Encoding Name	Clock Rate (Hz)
H263-1998	90,000

default

Specifies that the default list of dynamic codecs is added to the allowed codecs list. Default dynamic codecs: H263 and AMR.

no dynamic-codec [*encoding_name* **] [** *clock_rate* **] [** *channels* **]**

Specifies that all dynamic codecs are removed from the allowed codecs list. If an *encoding_name* is specified, then only the codec specified by the *encoding_name* is removed. Furthermore, if a supporting *clock_rate* and/or *channels* are specified, then only the *encoding_name* with the specified *clock_rate* and/or *channels* is removed.

Usage

Use this commands to create a list of supported dynamic audio and video codecs in the system. When a request is received by the CSCF, the SDP fields in the message are checked to determine the codec being used. The codec in the SDP fields must match a codec in the allowed codec list or the CSCF rejects the request.

Example

The following command adds the GSM-EFR codec to the allowed dynamic codec list:

```
dynamic-codec GSM-EFR
```

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

exit

Usage

Return to the previous mode.

static-codec

Creates a list of static codecs supported by the system.

Product

SCM

Privilege

Administrator

Syntax

```
static-codec { audio payload_type | video payload_type }

default static-codec

no static-codec [ payload_type ]
```

---

audio *payload_type* **| video** *payload_type*

audio *payload_type:* Specifies the audio codec added to the allowed codecs list. *payload_type* must be an integer from 0 to 95. Default value is 5.

Valid static audio codecs:

0: PCMU	7: LPC	14: MPA	21: unassigned
1: reserved	8: PCMA	15: G728	22: unassigned
2: reserved	9: G722	16: DVI4	23: unassigned
3: GSM	10: L16	17: DVI4	
4: G723	11: L16	18: G729	
5: DVI4	12: QCELP	19: reserved	
6: DVI4	13: CN	20: unassigned	

video *payload_type:* Specifies the video or audio-video codec added to the allowed codecs list. *payload_type* must be an integer from 0 to 95. Default value is 5.

Valid static video codecs:

24: unassigned	28: nv	32: MPV	72-76: reserved
25: CelB	29: unassigned	33: MP2T	77-95: unassigned
26: JPEG	30: unassigned	34: H263	
27: unassigned	31: H261	35-71: unassigned	

---

default

Specifies that the default list of static codecs is added to the allowed codecs list.
The default static codec is 5: DVI4.

no static-codec [*payload_type* **]**

Specifies that all static codecs are removed from the allowed codecs list. If a *payload_type* is specified, then only the codec specified by the *payload_type* is removed.

Usage

Use this commands to create a list of supported static audio and video codecs in the system. When a request is received by the CSCF, the SDP fields in the message are checked to determine the codec being used. The codec in the SDP fields must match a codec in the allowed codec list or the CSCF rejects the request.

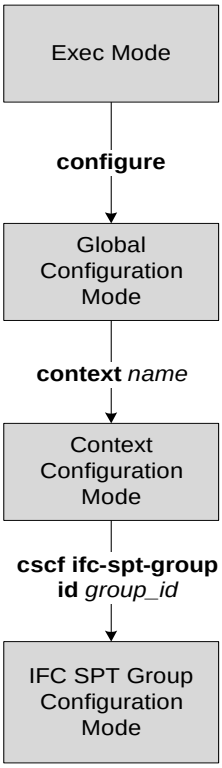
Example

The following command adds the G729 audio codec to the allowed codecs list:

```
static-codec 18
```

Chapter 73
CSCF IFC SPT Group Mode Commands

The CSCF iFC SPT Group Configuration Mode is used to associate individual SPT conditions with an Initial Filter Criteria (iFC) Service Point Trigger (SPT) group.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

exit

Usage

Return to the previous mode.

spt-condition

Assigns iFC SPT conditions to an existing iFC SPT group.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

`[ no ] spt-condition id` *`cond_id`*

`no`

Removes the specified CSCF iFC SPT condition from the iFC SPT group.

`spt-condition id` *`cond_id`*

Specifies the name of an existing iFC SPT condition.
`cond_name` must be an integer from 1 to 200.

Usage

Use this command to associate individual SPT conditions with an iFC SPT group.

Important: An iFC SPT group may be associated with multiple SPT conditions.

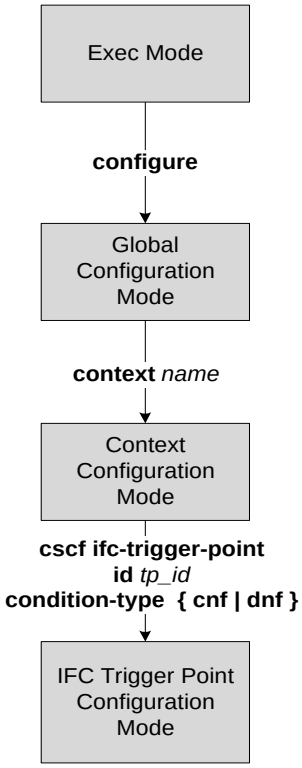
Example

The following command assigns 2 to an iFC SPT group:

```
spt-condition id 2
```

Chapter 74
CSCF IFC Trigger Point Mode Commands

The CSCF iFC Trigger Point Configuration Mode is used to associate an Initial Filter Criteria (iFC) Service Point Trigger (SPT) group with an iFC trigger point.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

exit

Usage

Return to the previous mode.

spt-group

Assigns an existing iFC SPT group to an iFC trigger point.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

[no] spt-group id *group_id*

no

Removes the specified CSCF iFC SPT group from the iFC trigger point.

spt-group id *group_id*

Specifies the ID of an existing iFC SPT group.
group_id must be an integer from 1 to 200.

Important: An iFC SPT group can be assigned to more than one iFC trigger point.

Usage

Use this command to associate an iFC SPT group with an iFC trigger point.

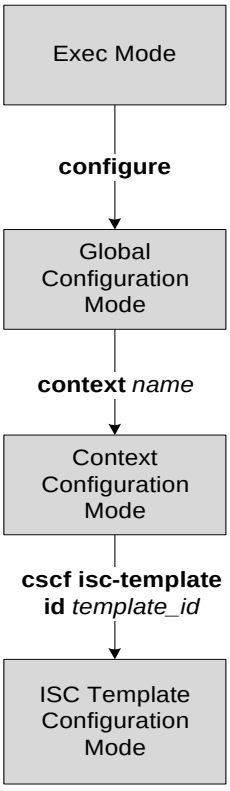
Example

The following command assigns iFC SPT group *2* to an iFC trigger point:

```
spt-group id 2
```

Chapter 75
CSCF ISC Template Configuration Mode Commands

The CSCF ISC Template Configuration Mode is used to configure the IMS Service Control (ISC) interface within the system.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

cnsa

Core Network Service Authorization (CNSA) related commands used to create media profile and service ids.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

cnsa { media-profile-id *profile_id* **| service-id** *service_id* **[** *service_id* **]...[** *service_id* **] }**

no cnsa { media-profile-id | service-id [*service_id* **] [** *service_id* **]...[** *service_id* **] }**

media-profile *profile_id*

Specifies the cnsa media profile id.
profile_id must be an integer from 0 to 10.
The media profile id is assigned to a service policy using the **cnsa-media-profile** command under CSCF Service configuration.

Important: You can only create one media profile id per ISC template.

service-id *service_id*

Specifies the cnsa service id(s). These ids represent URN parameters which are ICSI (IMS Communication Service Identifier) values that are mapped to a service profile through a media profile id.
service_id must be from 1 to 79 alpha and/or numeric characters.

no cnsa { media-profile-id | service-id [*service_id* **] [** *service_id* **]... [** *service_id* **] }**

Removes a media profile or service id(s).

Usage

Use this command to configure cnsa media profile ids and service ids. Information for core network authorization is received from HSS. It contains a list of service ids and a media profile id. Since the media profile id is an integer value, the S-CSCF needs to have a static database that contains the mapping between the integer value and the subscribed media profile. The media profile id is assigned to this service policy using the **cnsa-media-profile** command under CSCF Service configuration.
The S-CSCF selects the service profile based on the media profile id set and the policies, such as enforce-codec-policy and video-sessions, will be matched with the incoming request. Other policies, if configured, will be ignored in this scenario.

Example

The following command defines the media profile id as 2:

```
cnsa media-profile-id 2
```

The following command defines several service ids:

```
cnsa service-id xxx:exampletelephony.version1 xxx:abc.com
```

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

exit

Usage

Return to the previous mode.

filter-criteria

Configure the filter criteria to be used by this template.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

[no] filter-criteria id *criteria_id*

no

Removes the specified filter criteria.

id *criteria_id*

Specifies the ID of existing filter criteria to be used by this template. The particular criteria applied to a subscriber will be based on the priority parameter.
criteria_id must be an integer from 1 to 200.

Important: Filter criteria can be assigned to more than one ISC template.

Usage

Use this command to configure the filter criteria to be used by this template.

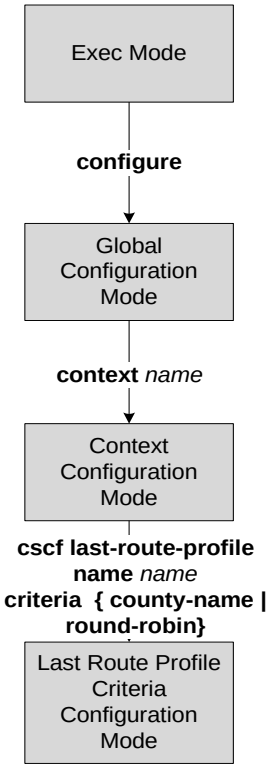
Example

The following command identifies the filter criteria *1*:

```
filter-criteria id 1
```

Chapter 76
CSCF Last Route Profile Criteria Configuration Mode Commands

The CSCF Last Route Profile Criteria Configuration Mode is used to configure county names and assign them Last Routing Option (LRO) numbers to be used by the CSCF last route profile. The S-CSCF forwards emergency call packets to the correct Public Safety Answering Point (PSAP) based on this criteria, which it receives from a peer server.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

county-name

Configure county names and assign them Last Routing Option (LRO) numbers to be used by the CSCF last route profile.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

county-name *county_name* **lro-number** *value*

[no] county-name *county_name*

county_name

Specifies the county name.
county_name must be from 1 to 79 alpha and/or numeric characters in length.

lro-number *value*

Specifies an existing LRO number.
value can be a maximum of ten digits in length.

no county-name *county_name*

Removes the specified county name.

Usage

Use this command to configure county names and assign them LRO numbers.

Important: You may configure up to 100 county names.

Example

The following command creates a county name called *norfolk* and assigns it an LRO number of *8884384357*:

```
county-name norfolk lro-number 8884384357
```

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

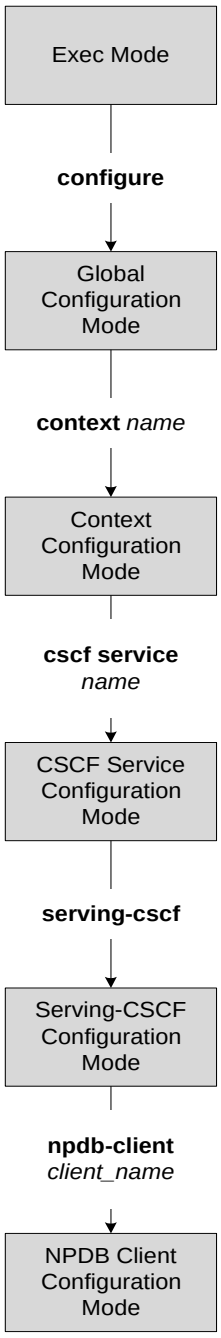
```
exit
```

Usage

Return to the previous mode.

Chapter 77
CSCF NPDB Client Configuration Mode Commands

The NPDB Client Configuration Mode is used to set various commands supporting the role of the NPDB (Number Portability Data Base) client. The NPDB client in a CSCF service performs query for called subscriber number on NPDB server, which returns the Routing Number for the query.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

bind

Binds the NPDB client to an IP address.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

bind address *IPv4_address* **system-id** *system_id* **id** *client_id* **[encrypted] password** *password*

no bind

address *IPv4_address*

Specifies the NPDB client IP address to establish the TCP connection with NPDB server.
IPv4_address must be expressed in dotted decimal notation for IPv4.

system-id *system_id*

Specifies the identifier of the system performing query to NPDB server.
system_id must be an unsigned integer from 0 to 4294962295.

id *client_id*

Specifies the ID of the NPDB client.
client_id must be from 1 to 15 alpha and/or numeric characters.

[encrypted] password *password*

Specifies the password of the NPDB client and whether it is encrypted.
password *password* must be from 1 to 15 alpha and/or numeric characters.
encrypted password *password* must be from 1 to 132 alpha and/or numeric characters.

Important: Normally, encrypted passwords are only used inside configuration files

no bind

Removes the binding of the NPDB client.

Usage

Use this command to establish the NPDB client parameters for TCP connection with NPDB server.

Important: This command can be entered multiple times to identify multiple IP addresses.

In connected state, only NPDB client will able to send query messages to get routing number from NPDB server. When query message is received in non-connected state from core, the NPDB client sends an error message to CSCF core.

Example

The following command binds the NPDB client to an IP address of *1.2.3.4*, system ID of *4294*, client ID of *asdds*, and encrypted password *A01h4b5t5rojj205dhrete*:

```
bind address 1.2.3.4 system-id 4294 id asdds encrypted password
A01h4b5t5rojj205dhrete
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

npdb-primary-server

Configure the NPDB primary server.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

npdb-primary-server { address *IPv4_address* **| domain** *domain* **} port** *port_number*

no npdb-primary-server

---

address *IPv4_address* **| domain** *domain*

Specifies the NPDB primary server.
address *IPv4_address*: IP addresses must be expressed in dotted decimal notation for IPv4.
domain *domain*: Domain name must be entered using from 1 to 255 alpha and/or numeric characters.

---

port *port_number*

Specifies the port at which NPDB primary server listens.
port_number may be an integer from 1024 to 65534.

---

no

Removes the NPDB primary server.

Usage

Use this command to configure the NPDB primary server.

Example

The following command adds an NPDB primary server with an IP address of *1.2.3.4* and a port number of *3878*:

```
npdb-primary-server address 1.2.3.4 port 3878
```

npdb-secondary-server

Configure the NPDB secondary server.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

npdb-secondary-server { address *IPv4_address* **| domain** *domain* **} port** *port_number*

no npdb-secondary-server

---

address *IPv4_address* **| domain** *domain*

Specifies the NPDB secondary server.
address *IPv4_address*: IP addresses must be expressed in dotted decimal notation for IPv4.
domain *domain*: Domain name must be entered using from 1 to 255 alpha and/or numeric characters.

---

port *port_number*

Specifies the port at which NPDB secondary server listens.
port_number may be an integer from 1024 to 65534.

---

no

Removes the NPDB secondary server.

Usage

Use this command to configure the NPDB secondary server.

Example

The following command adds an NPDB secondary server with an IP address of *1.2.3.5* and a port number of *3878*:

```
npdb-secondary-server address 1.2.3.5 port 3878
```

timeout

Sets timeout values for NPDB client.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

timeout { bind-response *sec* **| error-response** *sec* **| idle** *sec* **| ping** *sec* **| ping-response** *sec* **| query-response** *sec* **| release-response** *sec* **| tcp-retry** *sec* **}**

[default | no] timeout { bind-response | error-response | idle | ping | ping-response | query-response | release-response | tcp-retry }

bind-response *sec*

Default: 30
This timer is used to specify the timeout for connection path creation in seconds.
sec must be an integer from 1 to 5000.

error-response *sec*

Default: 30
This timer is used to specify the timeout for error response in seconds.
sec must be an integer from 1 to 5000.

idle *sec*

Default: 30
This timer is used to specify the timeout interval for retrying failed NPDB BIND in seconds.
sec must be an integer from 1 to 5000.

ping *sec*

Default: 20
This timer is used to specify the timeout to send ping message to make the connection alive in seconds.
sec must be an integer from 1 to 5000.

ping-response *sec*

Default: 30
This timer is used to specify the timeout for ping response in seconds.
sec must be an integer from 1 to 5000.

query-response *sec*

Default: 6
This timer is used to specify the timeout for query response in seconds.
sec must be an integer from 1 to 5000.

release-response *sec*

Default: 30
This timer is used to specify the timeout for release response in seconds.
sec must be an integer from 1 to 5000.

tcp-retry *sec*

Default: 15
This timer is used to specify the timeout interval for retrying failed TCP connection in seconds.
sec must be an integer from 1 to 5000.

default

Returns the command to the default settings. See keywords above for specific defaults.

no

Deletes the value configured for the specified timer.

Usage

Use this command to configure timeout values for NPDB client.
When CSCF service is started, NPDB client establishes TCP connections with NPDB primary and secondary servers (if configured) and sets the connection path by sending Bind message to server. If NPDB client fails to establish TCP connection to either of the servers, it will retry the connection every TCPRetryTimer interval until it is successful. When the connection is successful, NPDB client will go to the connected state and will start PingTimer. Whenever NPDB client receives service request from CSCF core, it sends the request based on the connected state of the server(s); it should always give higher preference to the primary server. When it fails to send a query message to server, NPDB client returns failure to the core. If both servers are not in connected state, NPDB client will send failure message to CSCF core.

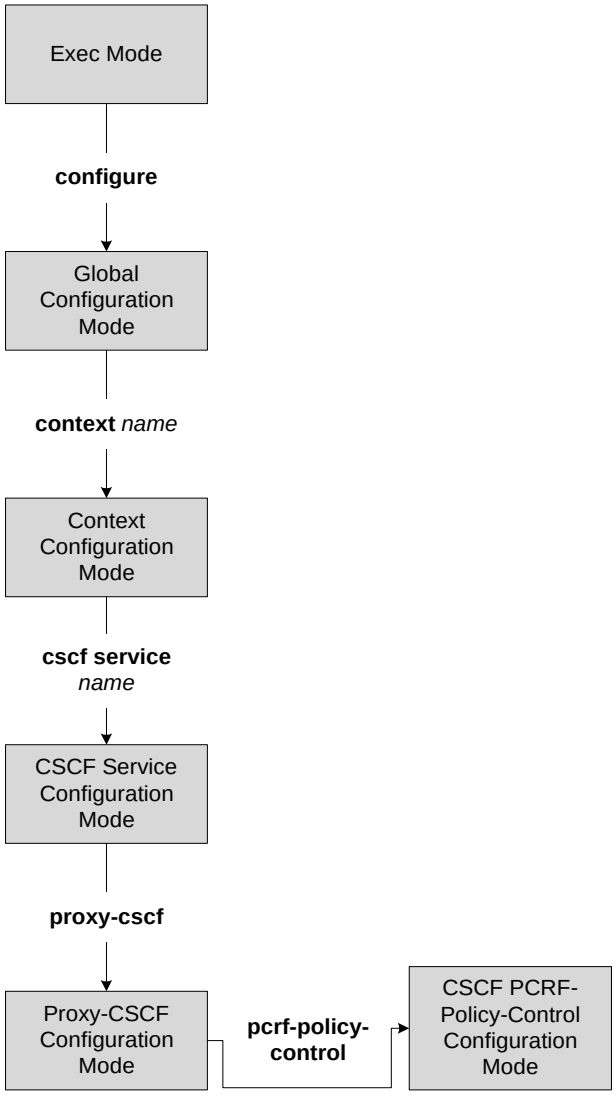
Example

The following command sets the release response timeout to *64* seconds:

```
timeout release-response 64
```

Chapter 78
CSCF PCRF-Policy-Control Configuration Mode Commands

The PCRF-Policy-Control Configuration Mode is used to enable PCRF policy control within the service.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

authorization mediatype

Enables media authorization, using external PCRF via Rx, of specific media types (present in the SDP of a SIP message) only.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ no ] authorization mediatype { application | audio | control | data | message | others
| text | video }
```

mediatype { application | audio | control | data | message | others | text | video }

Enables the external authorization of calls for the following SDP media types:

- **application**
- **audio**
- **control**
- **data**
- **message**
- **others**
- **text**
- **video**

no

Disables external authorization for the specified media type.

Usage

As Per 3GPP 29.214V8.5, P-CSCF/A-BG will authorize VOIP calls only for the media types enabled via this command. The P-CSCF/A-BG sends all media information for all supported media types present in SDP in AAR message to PCRF via Rx. For the other (unsupported) media types, P-CSCF will not send media information in AAR.
Be default, media authorization for all the media types is enabled.

Example

Enables the P-CSCF to authorize calls for audio media types:

```
authorization mediatype audio
```

Disables the authorization of calls for audio media types:

```
no authorization mediatype audio
```

authorization policy-interworking-failure

Allows/rejects a session based on configuration in case of failure from PCRF.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

authorization policy-interworking-failure { session-continue | session-reject [response-code *code* **])**

default authorization policy-interworking-failure

session-continue

P-CSCF continues session in case of failure from PCRF.

session-reject

P-CSCF rejects session in case of failure from PCRF.

response-code *code*

Specifies SIP response code for rejected session.
number must be an integer from 400 to 699. Default is 500.

default

By default, **session-reject** is activated to reject session with default response code 500.

Usage

Use this command to configure for policy interworking failure. Allow or reject a session based on configuration in case of failure from PCRF.

Example

The following command rejects session in case of failure from PCRF with SIP response code *450*:

```
authorization policy-interworking-failure session-reject response-code
450
```

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

exit

Usage

Return to the previous mode.

signaling-bearer-loss

Enables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification. This command is enabled by default.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ no ] signaling-bearer-loss subscription
```

no

Disables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification.

subscription

Enables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification.

Usage

Use this command to enable or disable subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification.
When enabled, the P-CSCF/A-BG sends AAR to the external PCRF via the Rx interface after UE registration. When disabled, the P-CSCF/A-BG will not subscribe to any event during Registration with PCRF and no diameter session will be established.

Example

Enables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification:

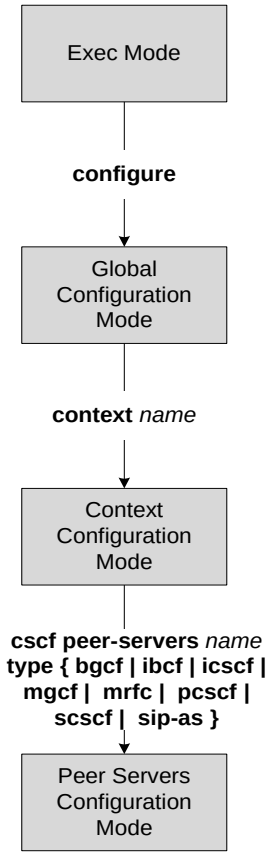
```
signaling-bearer-loss subscription
```

Disables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification:

```
no signaling-bearer-loss subscription
```

Chapter 79
CSCF Peer Servers Configuration Mode Commands

The CSCF Peer Servers Configuration Mode is used to configure peer servers (for next-hop session routes) within the system.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

exit

Usage

Return to the previous mode.

hunting-method

Configures the method by which server is contacted.

Product

SCM

Privilege

Administrator

Syntax

```
hunting-method { round-robin | sequence-on-failure | weighed }

default hunting-method
```

round-robin | sequence-on-failure | weighed

Specifies the hunting method for the server.
round-robin: Specifies that the server will be used in round-robin fashion. This is the default setting.
sequence-on-failure: Specifies that the server will be used sequentially if a failure occurs on a server (i.e., first peer server is always used, except on failure, during which next peer server in the list will be used).
weighed: Specifies that the peer server has a set "weight" that determines use as compared to the other like-configured peer servers. The actual weight of the peer server is configured in the **server** command in this mode.

default

Specifies that the server will be used in round-robin fashion.

Usage

Use this command to configure the method that is used by the system to connect to the peer server.

Example

The following command sets the hunting method for a server to contact sequentially only when a server fails:

```
hunting-method sequence-on-failure
```

server

Configures the name, IP address, and port of servers belonging to this peer server and enters the Server Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

server *name* **{ address** *ip_address* **| domain** *domain_name* **} [port** *number* **] [transport { tcp | udp }] [weight** *number* **]**

no server *name*

name

Specifies a name for the server. *name* must be from 1 to 79 alpha and/or numeric characters in length.

address *ip_address*

Specifies the IP address of the server. *ip_address* is expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

domain *domain_name*

Specifies the domain name of the peer server. *domain_name* must be from 1 to 255 alpha and/or numeric characters in length.

port *number*

Specifies the port number of the server.
number must be an integer value from 1 to 65535.

transport { tcp | udp }

Specifies the transport type (TCP or UDP).

weight *number*

Default: 5
Specifies a weighted number for the specific peer server for load balancing purposes. *number* must be an integer value from 1 to 10. Higher weight implies larger server capability (and more routed requests).

Important: This keyword is only valid if the **weighed** keyword is applied to the **hunting-method** command in this mode.

no server *name*

Removes the specified server from the group.

Usage

Use this command to configure servers and enter the Server Configuration Mode.
Entering this command results in the following prompt:

```
[context_name]hostname(config-server_name-peer-server)#
```

Server Configuration Mode commands are defined in the *CSCF Peer Server Monitoring Configuration Mode Commands* chapter.

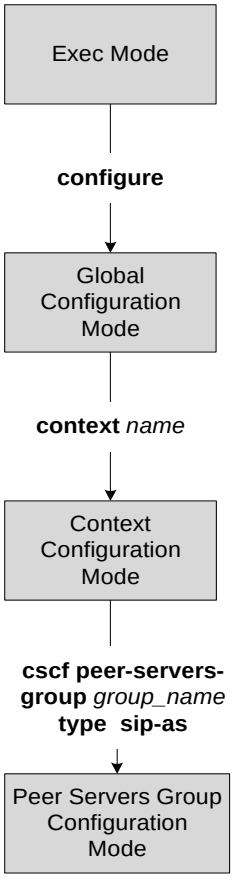
Example

The following command configures a server named *scscf5* with an IP address of *1.2.3.4* and a port number of *5060*:

```
server scscf5 address 1.2.3.4 port 5060
```

Chapter 80
CSCF Peer Servers Group Configuration Mode Commands

The CSCF Peer Servers Group Configuration Mode is used to configure peer servers lists within a peer servers group.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

peer-servers

Configures peer servers lists in the peer servers group.

Product

SCM

Privilege

Administrator

Syntax

peer-servers *list_name* **{ default | mode { active | standby } }**

no peer-servers *list_name*

list_name

Specifies a name for the peer servers list. *list_name* must be from 1 to 79 alpha and/or numeric characters in length.

default

Specifies that the peer servers list is default.

mode { active | standby }

Specifies whether the peer servers list is active or standby.

no peer-servers *list_name*

Removes the specified peer servers list from the group.

Usage

Use this command to manage peer servers lists in a peer servers group.

Important: There can be one active, one standby, and one default peer servers list in a peer servers group.

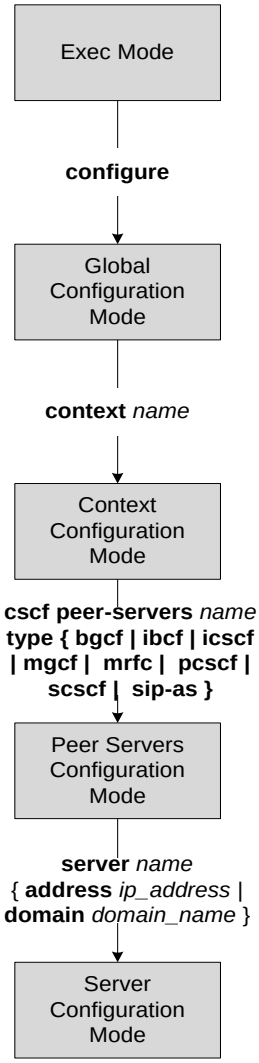
Example

The following command configures an active peer servers list named *active_as_list*:

```
peer-servers active_as_list mode active
```

Chapter 81
CSCF Peer Server Monitoring Configuration Mode Commands

The CSCF Peer Server Monitoring Configuration Mode is used to configure an individual peer server's monitoring parameters and operational mode. It also associates a network session template with the server.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

dummy-as

Sets a response code for Dummy-AS peer server.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

dummy-as custom-response-code *SIP_response_code*

default dummy-as custom-response-code

custom-response-code *SIP_response_code*

If the peer server is configured as dummy-as and it is chosen as per routing table configured, a UMM response message will be formed with the response code configured and sent as reply to incoming MESSAGE/PUBLISH requests.
SIP_response_code must be an integer from 200 to 699.

Important: The response code can be 2xx/4xx/5xx/6xx; 3xx,401,and 407 are not allowed.

default dummy-as custom-response-code

Sets the response code to 200.

Usage

Use this command to configure a response code for Dummy-AS. If this mode is selected, then MESSAGE/PUBLISH requests will be responded to by S-CSCF with configured response code.

Example

The following command configures AS as Dummy-AS with a corresponding response code of *425*:

```
dummy-as custom-response-code 425
```

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

```
exit
```

Usage

Return to the previous mode.

ims-capable

Indicates whether the peer server belongs to a 3GPP/IMS network or a non-IMS network such as the Internet. This command is used to determine at the S-CSCF whether SIP signaling inter-working is needed when the calls are forwarded to external networks.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
[ no ] ims-capable
```

no

Removes the identification of "IMS capable" from the selected peer server.

Usage

Use this command to identify a peer server as IMS capable allowing the S-CSCF to use SIP signalling inter-working when forwarding calls to non-IMS capable networks.

lro-selection-profile

Binds a CSCF last route profile with the peer server.

Product

SCM

Privilege

Administrator

Syntax

lro-selection-profile name *profile_name*

no lro-selection-profile

lro-selection-profile name *profile_name*

profile_name must be an existing CSCF last route profile and be from 1 to 79 alpha and/or numeric characters.

no lro-selection-profile

Removes CSCF last route profile from the peer server group.

Usage

Use this command to identify a CSCF last route profile to use for finding the correct Public Safety Answering Point (PSAP) during emergency calls.

Example

The following command assigns a CSCF last route profile named *lro1* to the peer server group:

```
lro-selection-profile name lro1
```

The following command removes a CSCF last route profile from the peer server group:

```
no lro-selection-profile
```

mode

Sets the peer server mode to either active or standby. By default, peer servers are in active mode.

Product

SCM

Privilege

Administrator

Syntax

```
mode { active | standby }
```

active

Defines the mode of the CSCF peer server as active.

standby

Defines the mode of the CSCF peer server as standby.

Usage

Use this command to set the peer server mode to either active or standby.

Example

The following command sets the peer server's mode to standby:

```
mode standby
```

monitor-status

Sets parameters for monitoring the status of peer servers.

Product

SCM

Privilege

Administrator

Syntax

```
monitor-status { max-response-codes negative max | [ monitor-interval seconds ] [
monitor-message options [ max-forwards max | response-timer seconds ] ] [ monitor-
response-timer seconds ] | response-code { positive SIP_response_code | negative
SIP_response_code } | timer [ mark-out-of-service seconds ] [ unavailable-monitor-
interval seconds ] [ unavailable-notification seconds ] }

no monitor-status { monitor | response-code [ negative | positive ] [ SIP_response_code ]
}
```

max-response-codes negative *max*

Default: 1
Specifies the maximum number of negative response codes to receive to mark server unavailable.
max must be an integer from 1 to 10.

monitor-interval *seconds*

Default: 30
Specifies the interval that peer server monitoring will occur.
seconds must be an integer from 1 to 65535.

monitor-message options [max-forwards *max* **| response-timer** *seconds* **]**

Specifies that SIP message (OPTIONS) are to be sent periodically after each monitoring interval.
max-forwards *max*: Max-forwards in number of hops. *max* must be an integer from 0 to 70.
response-timer *seconds*: Response wait timer in seconds. *seconds* must be an integer from 1 to 65535.

monitor-response-timer *seconds*

Default: 180
Specifies the interval that the CSCF will wait for responses from the peer server.
seconds must be an integer from 1 to 65535.

response-code { positive *SIP_response_code* **| negative** *SIP_response_code* **}**

Specifies the Options Message response codes.
negative: Negative response codes. *SIP_response_code* must be an integer from 300 to 699.
positive: Positive response codes. *SIP_response_code* must be an integer from 200 to 299.

timer mark-out-of-service *seconds*

Default: 864000
Timer to mark server out-of-service from unavailable state.

seconds must be an integer from 0 to 2147483646.

timer unavailable-monitor-interval *seconds*

Periodic monitor interval to be used when server is marked as unavailable.
seconds must be an integer from 0 to 2147483646.

timer unavailable-notification *seconds*

Default: 180
Time after which to send notification to operations administrator.
seconds must be an integer from 0 to 2147483646.

no monitor-status { monitor | response-code [negative | positive] [*SIP_response_code* **] }**

Disables peering server status monitoring.

Usage

Use this command to set parameters for monitoring the status of a peer server.

Example

The following command sets the monitoring interval to three minutes (*180* seconds) and the response timer to six minutes (*360* seconds):

```
monitor-status monitor-interval 180 monitor-response-timer 360
```

nw-session-template

Specifies a session template for sessions terminating from the peer server group.

Product

SCM

Privilege

Administrator

Syntax

nw-session-template name *template_name*

no nw-session-template

name *template_name*

template_name must be an existing session template created in the Session Template Configuration Mode.

no

Removes session template from the peer server group.

Usage

Use this command to identify a session template to use for sessions terminating from the peer server group.

Example

The following command identifies a session template named *template-25* to use for sessions terminating from the peer server group:

```
nw-session-template template-25
```

registration

This command specifies whether the S-CSCF skips third party registration to the Application Server (AS) by a configured time after initial registration.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

registration skip-count *count*

no registration skip-count

skip-count *count*

Number of times to skip third party registration.
count must be an integer from 0 (default) to 60.

no registration skip-count

The S-CSCF does not skip third party registration to the AS by a configured time after initial registration.

Usage

Use this command to specify whether the S-CSCF skips third party registration to the Application Server (AS) by a configured time after initial registration. After skipping the configured number of times, the third party register should be sent again to AS to reduce overload on AS.

Example

The following command sets the number of times to skip third party registration to *25*:

```
registration skip-count 25
```

tps-rate

Controls the rate of messages based on Transactions Per Second (TPS) from S-CSCF towards the peer server application server (AS).

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
tps-rate rate [ exclude Register ]

no tps-rate
```

rate

TPS from S-CSCF towards the peer server AS.
rate must be an integer from 1 to 1000.

exclude Register

Specifies that for Register method, TPS rate need not be applied.

no

TPS rate not applied from S-CSCF towards the peer server AS.

Usage

Use this command to control the TPS towards the peer server AS. If TPS rate is exceeded, the incoming requests will be rejected with 500 error response; Retry-After Header specifies the number of seconds before UE should retry.

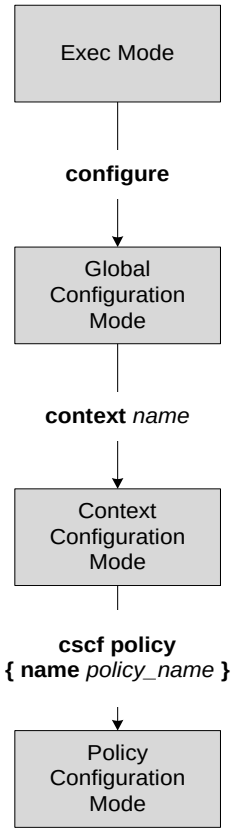
Example

The following command sets the TPS rate towards the AS to *25*:

```
tps-rate 25
```

Chapter 82
CSCF Policy Configuration Mode Commands

The CSCF Policy Configuration Mode is used to manage AoR policy profiles within the system. User-defined profiles can be managed in this mode.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

aor-policy-rules

Specifies that the newly created policy is an AoR policy and enters the AoR Policy Rules Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

```
aor-policy-rules
```

Usage

Use this command to create an AoR policy group and enter the AoR Policy Rules Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-aor-policy)#
```

AoR Policy Configuration Mode commands are defined in the *CSCF AoR Policy Rules Configuration Mode Commands* chapter.

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

```
exit
```

Usage

Return to the previous mode.

service-policy-rules

Specifies that the newly created policy is a service policy and enters the Service Policy Rules Configuration Mode.

Product

SCM

Privilege

Administrator

Syntax

```
service-policy-rules
```

Usage

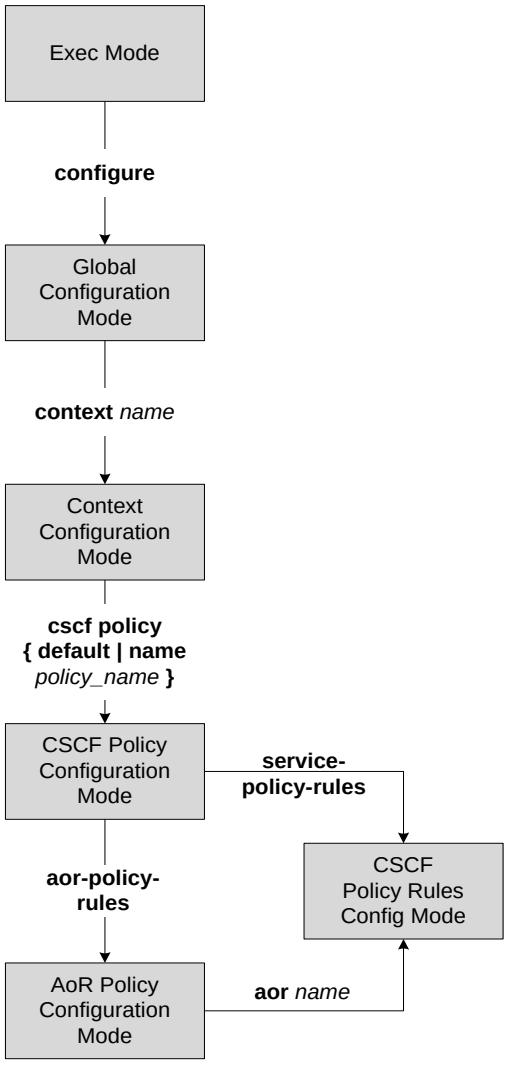
Use this command to create a service policy group and enter the CSCF Policy Rules Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-service-policy)#
```

Service Policy Rule Configuration Mode commands are defined in the *CSCF Policy Rules Configuration Mode Commands* chapter.

Chapter 83
CSCF Policy Rules Configuration Mode Commands

The CSCF Policy Rules Configuration Mode is used to manage CSCF AoR and service policy profiles within the system.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

allow-noauth

Configures the policy to allow unauthenticated access. Default is disabled.

Product

SCM

Privilege

Administrator

Syntax

```
[ default | no ] allow-noauth
```

default | no

Disables the allow-noauth functionality for this policy.

Usage

Use this command to allow access to subscribers without authenticating them.

allow-unsecure

Configures the policy to allow access to the system without a security association. Default is disabled.

Product

SCM

Privilege

Administrator

Syntax

```
[ default | no ] allow-unsecure
```

default | no

Disables the allow-unsecure functionality for this policy.

Usage

Use this command to enable the policy to provide subscriber access to system without a security association.

authorization

Configures the policy to allow early bandwidth or provisional response authorization. Default is disabled.

Product

SCM

Privilege

Administrator

Syntax

```
[ default | no ] authorization { early-bandwidth | prov-response }
```

early-bandwidth

Enables early bandwidth policy.

prov-response

Enables AAR for provisional responses like 18X.

default | no

Disables the early bandwidth or provisional response authorization functionality for this policy.

Usage

Use this command to enable the policy to provide early bandwidth or provisional response authorization.

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

enforce-codec-policy

Enters the Enforce Codec Policy Command Mode where allowed static and dynamic codec lists are managed.

Product

SCM

Privilege

Administrator

Syntax

```
[ default | no ] enforce-codec-policy
```

default | no

Disables the codec policy.

Usage

Use this command to enter the Enforce Codec Policy Configuration Mode.
Entering this command results in the following prompt:

```
[context_name]hostname(config-policy-enforce-codec)#
```

CSCF Enforce Codec Policy Mode commands are defined in the *Enforce Codec Policy Configuration Mode Commands* chapter in this guide.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

exit

Usage

Return to the previous mode.

max-cscf-concurrent-sessions

Configures the maximum number of concurrent sessions allowed per subscriber.

Product

SCM

Privilege

Administrator

Syntax

max-cscf-concurrent-sessions *number*

default max-cscf-concurrent-sessions

number

Default: 5
Specifies the number of concurrent sessions allowed per subscriber for this policy. *number* must be an integer from 1 to 100.

default

Resets defaults for this command.

Usage

Use this command to set the maximum number of allowed sessions per subscriber for this policy.
If enabled, the **subscriber-policy-override** command in the CSCF Service Configuration Mode overrides the service-level policy.

Example

The following command sets the maximum number of concurrent sessions for a subscriber using this policy to 7:

```
max-cscf-concurrent-sessions 7
```

policy

Configures the overload response for this policy. When the P-CSCF/A-BG becomes congested, this overload policy is used to reject subsequent sessions or redirect them to another server.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
policy overload { redirect address1 [ weight weight1 ] [ address2 [ weight weight2 ] ]
... | reject [ use-reject-code { admin-prohibited | insufficient-resources } ] }

default policy overload

no policy overload redirect address1[address2] ...
```

redirect *address1* **[weight** *weight1* **] [** *address2* **[weight** *weight2* **]] ...**

Specifies that upon policy overload, the system will redirect the session to another CSCF.
address1 must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
weight *weight1*: Defines the priority of the redirect address.
weight1 must be an integer from 1 to 10. Default is 1.

reject [use-reject-code { admin-prohibited | insufficient-resources }]

Specifies that upon policy overload, the system will reject the session. This is the default setting.
use-reject-code: Specifies that a reject code will be returned upon policy overload.

- **admin-prohibited**: Specifies that the "admin-prohibited" reject code will be returned upon policy overload.
- **insufficient-resources**: Specifies that the "insufficient resources" reject code will be returned upon policy overload. This is the default reject code.

default policy overload

Resets defaults for this command.

no policy overload redirect *address1* **[** *address2* **] ...**

Removes configured policy overload redirect address(es).

Usage

Use this command to define the response to an overload condition on the P-CSCF/A-BG using this AoR policy.

Example

The following command configures the policy overload response to redirect to a series of CSCFs with IP address of *1.2.3.4*, *1.2.3.5*, and *1.2.3.6* with respective priorities (weights) of *1*, *3*, and *2*:

```
policy overload redirect 1.2.3.4 weight 1 1.2.3.5 weight 3 1.2.3.6 weight
2
```

qos

Configures QoS bandwidth settings for uplink and downlink.

Product

SCM

Privilege

Administrator

Syntax

qos bandwidth { downlink| uplink } [peak *value* **]**

bandwidth { downlink| uplink }

downlink: Configures the downlink bandwidth.
uplink: Configures the uplink bandwidth.

peak *value*

Peak value of bandwidth in kilobits per second (kbit/s).
value must be an integer from 1 to 99999999.

Usage

The P-CSCF/A-BG fills the required bandwidth for downlink and uplink from the Session Description Protocol (SDP) in the message when communicating with an external policy server via Rx/Tx/Gq. Use this command to configure the peak uplink and downlink bandwidth to be used when the SDP does not contain bandwidth.

Example

Set the peak uplink bandwidth to *256* kbit/s:

```
qos bandwidth uplink peak 256
```

video-sessions

Configures the policy to allow video bearers. Default is disabled.

Product

SCM

Privilege

Administrator

Syntax

```
[ default | no ] video-sessions
```

default | no

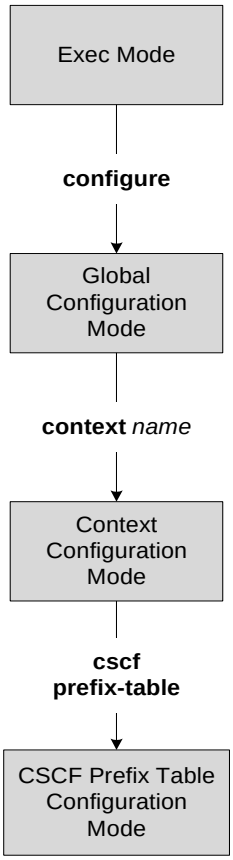
Disables the “allow video sessions” feature.

Usage

Use this command to allow video session via this policy.

Chapter 84
CSCF Prefix Table Configuration Mode Commands

The CSCF prefix table is used to configure for each number (or number prefix) whether it is ported and the SIP routing domain. Only one CSCF prefix table can be configured per context.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

number

Determines for each number (or number prefix) in a prefix table whether it is ported and the SIP routing domain.

Product

SCM

Privilege

Administrator

Syntax

number *number* **[ported] [routing-domain** *domain_name* **]**

no number *number*

number

Specifies number or number prefix. *number* must be a string of digits from 1 to 31 and/or special character "$."

Important: If the number is a prefix, it should end with "$."

ported

The number (or number prefix) is in ported range and NPDB (Number Portability Data Base) has to be contacted.

routing-domain *domain*

Specifies the SIP routing domain for this number (or number prefix). *domain_name* must be from 1 to 79 alpha and/or numeric characters in length.

no number *number*

Removes the specified number or number prefix from the prefix table.

Usage

Use this command to determine whether each number (or number prefix) in a prefix table is ported and the SIP routing domain. The S-CSCF service will use the prefix table configured in its source context for the lookup.

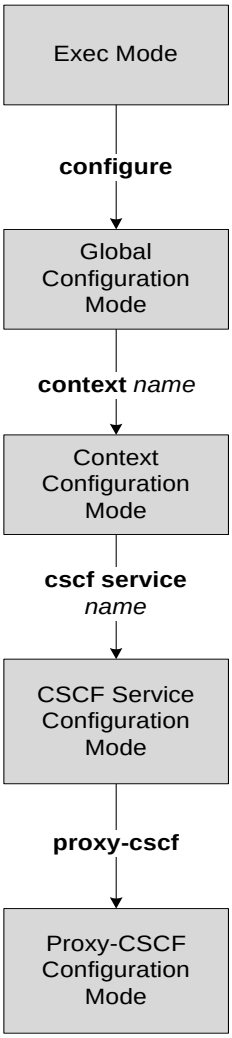
Example

The following command specifies a ported number prefix named *821057$.* with SIP routing domain *cisco.com*:

```
number 821057$ ported routing-domain cisco.com
```

Chapter 85
CSCF Proxy-CSCF Configuration Mode Commands

The Proxy-CSCF Configuration Mode is used to enable Diameter policy control within the service.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

allow rfc3261-ua-interworking

Enables the function to allow IMS interworking with RFC3261 SIP User Agents.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ no ] allow rfc3261-ua-interworking
```

no

Disables the interworking capability.

Usage

Use this command to enable the P-CSCF/A-BG to allow IMS interworking with RFC3261 SIP User Agents.

core-reg-expiry-time

Configures Registration Expiry Timer Handling in P-CSCF/A-BG to keep pin holes open in B2BUA mode.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

core-reg-expiry-time *sec*

[default | no] core-reg-expiry-time

sec

Expiry age should be less than or equal to the maximum in seconds. Must be an integer from 300 to 86400.

default

Sets the core-reg-expiry-time to 3600 seconds.

no

Disables the timer.

Usage

Use this command to configure Registration Expiry Timer Handling in P-CSCF/A-BG to keep pin holes open in B2BUA mode.

Example

The following sets the core-reg-expiry-time to *4000* seconds:

```
core-reg-expiry-time 4000
```

diameter

This command:

- configures the Diameter dictionary used in this function.
- configures the policy control origin endpoint used in this function.
- enables the selection of a Diameter policy control peer server providing Rx/Tx/Gq applications for this service.
- configures the Diameter requested timeout value used in this function.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

diameter location-info { dictionary { e2custom01 | e2custom02 | e2custom03 | e2custom04 | e2custom05 | e2custom06 | e2custom07 | e2custom08 | e2custom09 | e2standard } | origin endpoint endpoint_name | peer-select peer *peer_name* **[peer-realm** *realm_name* **] [secondary-peer** *peer_name* **[sec-peer-realm** *realm_name* **]] | request-timeout** *sec* **}**

diameter policy-control { dictionary { Gq-custom | Gq-standard | Rq-custom| Rx-rel8 | Rx-standard | Tx-standard | custom01 | custom02 | custom03 | custom04 | custom05 | custom06 | custom07 | custom08 | custom09 } | origin endpoint endpoint_name | peer-select peer *peer_name* **[peer-realm** *realm_name* **] [secondary-peer** *peer_name* **[sec-peer-realm** *realm_name* **]] | request-timeout** *sec* **}**

In StarOS v12.2 and later:

diameter policy-control { dictionary { gq-custom | gq-standard | rq-custom | rx-custom01 | rx-custom02 | rx-custom03 | rx-custom04 | rx-custom05 | rx-rel8 | rx-standard | tx-standard } | origin endpoint endpoint_name | peer-select peer *peer_name* **[peer-realm** *realm_name* **] [secondary-peer** *peer_name* **[sec-peer-realm** *realm_name* **]] | request-timeout** *sec* **}**

default diameter { location-info | policy-control } { **dictionary | request-timeout }**

no diameter { location-info | policy-control } [origin endpoint | peer-select]

---

location-info

Defines the E2 interface for location information.

---

dictionary { e2custom01...e2custom09 | e2standard }

custom01...custom09: Specifies that a customer-specific (custom) dictionary is to be used for expansion and behaviors.
e2standard: Specifies that the E2-Standard-Dictionary is to be used.

Important: If this keyword is not configured, the system defaults to the default dictionary (e2standard). In the Proxy-CSCF configuration, at any time, the location-info dictionary can either be an explicitly configured dictionary or the default dictionary. Hence, there is no corresponding "no" CLI to disable the location-info dictionary setting.

policy-control

Defines external policy control.

dictionary { Gq-custom | Gq-standard | Rq-custom | Rx-rel8 | Rx-standard | Tx-standard | custom01...custom09 }

Gq-custom: Specifies that the Gq Operax dictionary is to be used for Operax-specific behavior.
Gq-standard: Specifies that the Gq standard dictionary is to be used.
Rq-custom: Specifies that the Rq custom dictionary is to be used.
Rx-rel8: Specifies that the Rx Release 8 dictionary is to be used.
Rx-standard: Specifies that the Rx standard dictionary is to be used.
Tx-standard: Specifies that the Tx standard dictionary is to be used.
custom01...custom09: Specifies that a customer-specific (custom) dictionary, for customer-specific expansion and behaviors, is to be used.

dictionary { gq-custom | gq-standard | rq-custom | rx-custom01 | rx-custom02 | rx-custom03 | rx-custom04 | rx-custom05 | rx-rel8 | rx-standard | tx-standard }

gq-custom : Specifies that the Gq Operax dictionary is to be used for Operax-specific behavior.
gq-standardd: Specifies that the Gq standard dictionary is to be used.
rq-custom: Specifies that the Rq custom dictionary is to be used.
rx-custom01...rx-custom05: Specifies that a customer-specific (custom) dictionary, for customer-specific expansion and behaviors, is to be used.
rx-rel8: Specifies that the Rx Release 8 dictionary is to be used.
rx-standard: Specifies that the Rx standard dictionary is to be used.
tx-standard: Specifies that the Tx standard dictionary is to be used.

origin endpoint *endpoint_name*

Specifies the Diameter location-info or policy control endpoint name.
endpoint_name must be the endpoint's name and an alpha and/or numeric string of 1 through 63 characters in length.

peer-select peer *peer_name*

Specifies the name of the Diameter location-info or policy control peer server.
peer_name must be from 1 to 63 alpha and/or numeric characters in length.
Diameter peer servers are configured through the **diameter endpoint** command in the Context Configuration Mode. The **diameter endpoint** command is a generic command and can be found in the Cisco ASR 5000 Series Command Line Interface Reference.

peer-realm *realm_name*

Specifies the realm name for which the Diameter location-info or policy control peer server has responsibility.
realm_name must be from 1 to 63 alpha and/or numeric characters in length.

Important: If this keyword is not configured, the system defaults to the realm name configured for the selected peer server.

`secondary-peer` *`peer_name`*

Specifies the name of the secondary Diameter location-info or policy control peer server.
`peer_name` must be from 1 to 63 alpha and/or numeric characters in length.

`sec-peer-realm` *`realm_name`*

Specifies the realm name for which the secondary Diameter location-info or policy control peer server has responsibility.
`realm_name` must be from 1 to 63 alpha and/or numeric characters in length.

Important: If this keyword is not configured, the system defaults to the realm name configured for the selected peer server.

Important: The "**`diameter location-info peer-select peer`** *`<primary_peer>`* **`peer-realm`** *`<primary_peer_realm>`* **`secondary-peer`** *`<secondary_peer>`* **`sec-peer-realm`** *`<secondary_peer_realm>`*" CLI configures Peer Switching—selecting which peers the Diameter messages are routed to. When the secondary peer is configured, in case the primary fails, request messages are rerouted to the secondary. Note that the "**`no diameter location-info peer-select`**" CLI command will remove the entire Peer Switching CLI from the configuration.

`request-timeout` *`sec`*

Specifies the Diameter location-info or policy control requested timeout value in seconds.
`sec` must be an integer from 1 to 300.
Default: 10

Important: If this keyword is not configured, the system defaults to the default setting (10 seconds). In the Proxy-CSCF configuration, at any time, the request-timeout setting can either be an explicitly configured value or the default value. Hence, there is no corresponding "no" CLI to disable the request-timeout setting.

`default`

Sets the Diameter's location-info or policy control dictionary or requested timeout value as the default.

`no`

Removes the Diameter location-info or policy control origin endpoint or Diameter peer from the service.

Usage

Use this command to:

- define the Diameter dictionary to use for the service.
- specify the Diameter origin endpoint.
- specify a Diameter location-info or policy control peer server to support Rx/Tx/Gq applications.
- specify the Diameter requested timeout value for this service.

Example

The following command configures the system to use the Tx standard Diameter dictionary for this service:

```
diameter policy-control dictionary Tx-standard
```

The following command sets the Diameter location-info origin endpoint to *test*:

```
diameter location-info origin endpoint test
```

The following command selects a Diameter policy control peer server with a name of *diam-2* and a realm name of *realm-6*:

```
diameter policy-control peer-select peer diam-2 peer-realm realm-6
```

emergency

Configures the function to allow or disallow the emergency-session or emergency-registration of a particular type.

Product

SCM (P-CSCF, A-BG, SIP Proxy)

Privilege

Administrator

Syntax

```
[ default | no ] emergency { registration [ visited-ue ] | session [ 3gpp-ims-xml-body |
anonymous | non-emergency-registered | sdp-cs-media | visited-ue ] }
```

default

Specifies that the emergency-session or emergency-registration of a particular type can be allowed.

no

Disallows the emergency-session or emergency-registration of a particular type.

registration [visited-ue]

Allow emergency-registration. By default, it's allowed.
visited-ue: Allow emergency-registration from a visited UE. By default, it's allowed.

session [3gpp-ims-xml-body | anonymous | non-emergency-registered | sdp-cs-media | visited-ue]

Specifies the type of emergency-session to be allowed or disallowed. By default, all are allowed.
3gpp-ims-xml-body: Allow 3GPP IM CN XML body to be added in 380 response messages.
anonymous: Allow anonymous subscribers (unregistered UEs) to initiate emergency sessions.
non-emergency-registered: Allow non-emergency registered subscribers to initiate emergency sessions.
sdp-cs-media: Allow emergency calls with SDP CS Media.
visited-ue: Allow emergency calls from visited UE.

Usage

Use this command to configure the function to allow or disallow the emergency-session or emergency-registration of a particular type.

Example

The following command configures the function to allow non-emergency registered subscribers to initiate emergency sessions:

```
emergency session non-emergency-registered
```

emergency-call-mode

Enables the P-CSCF/A-BG service to add “P-Emergency-Call-Mode-Preference” header in 200OK to REGISTER message. By default, this command is disabled.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
emergency-call-mode { 3gpp-cs | 3gpp-ims }

[ default | no ] emergency-call-mode
```

3gpp-cs | 3gpp-ims

3gpp-cs: Specifies 3GPP CS access preference in header.
3gpp-ims (default): Specifies 3GPP IMS access preference in header.

default

Specifies 3GPP IMS access preference in header.

no

Disables “P-Emergency-Call-Mode-Preference” header insertion for the P-CSCF/A-BG service.

Usage

Enabling this command allows the P-CSCF or A-BG to add a “P-Emergency-Call-Mode-Preference” header in 200OK to REGISTER message.

Example

The following command enables “P-Emergency-Call-Mode-Preference” header insertion with a 3GPP CS access preference defined:

```
emergency-call-mode 3gpp-cs
```

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

exit

Usage

Return to the previous mode.

interrogating-cscf-role

Enables the function to also perform as an Interrogating-CSCF.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ no ] interrogating-cscf-role
```

no

Disables the Interrogating-CSCF role in this function.

Usage

Use this command to enable the P-CSCF/A-BG to also perform as an Interrogating-CSCF.

Important: All Interrogating-CSCF functions have been moved to the Serving-CSCF exclusively in v10.0 and beyond.

message-max-size

Configures the maximum message body size in MESSAGE method.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

message-max-size *limit*

[default | no] message-max-size

limit

Default: 1024
Configures the maximum SIP message size limit in bytes for any SIP message buffer.
limit must be an integer from 512 to 65535.

Important: Message body size should be less than the max-sipmsg-size set in the CSCF Service Configuration Mode.

default | no

Returns/sets the maximum SIP message size to 1024 bytes.

Usage

Use this command to configure the maximum SIP message size for any SIP message buffer.

Example

The following command limits the SIP message size to *4000* bytes:

```
message-max-size 4000
```

network-id

Configures the Network Identifier.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

[no] network-id *id*

no

Removes the configured Network Identifier of the entity.

id

The Network Identifier of the entity.
id must be from 1 to 79 alpha and/or numeric characters in length.

Usage

The Network Identifier is used by the P-CSCF or A-BG to fill the P-Visited-Network-ID header.

Example

Sets the Network Identifier to *pcscf01.company.com:*

```
network-id pcscf01.company.com
```

pcrf-policy-control

Enables enables external policy control via PCRF through the Rx Diameter interface and enters the PCRF-Policy-Control Configuration Mode. Default is disabled.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ no ] pcrf-policy-control
```

no

Disables external policy control via PCRF for this service. P-CSCF/A-BG will not establish any Diameter session with PCRF, even though the PCRF is configured. This option disables both authorization and subscription to PCRF during Registration and VOIP call.

Usage

Use this command to enable PCRF policy control and enter the PCRF-Policy-Control Configuration Mode. It enables authorization and subscription to PCRF during Registration and VOIP calls. If the P-CSCF cannot connect to the PCRF server (due to wrong configuration in CSCF or PCRF unavailability), then P-CSCF/A-BG does not authorize media and VOIP calls will be rejected due to auth failure. Registrations will be handled normally.
Entering this command results in the following prompt:

```
[context_name]hostname(config-pcrf-policy-control)#
```

PCRF-Policy-Control Configuration Mode commands are defined in the *CSCF PCRF-Policy-Control Configuration Mode Commands* chapter in this guide.

peer-sbc

Configures peer Session Border Controller (SBC) addresses from where the P-CSCF/A-BG service can receive requests.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

[no] peer-sbc *ip_address*

no

Removes the IP address of a peer SBC from this P-CSCF/A-BG service.

ip_address

Specifies the IP address of a peer SBC for this P-CSCF/A-BG service.
ip_address is expressed in standard dotted decimal notation for IPv4 or colon notation for IPv6.

Usage

Use this command to specify peer Session Border Controller (SBC) addresses from where the P-CSCF/A-BG service can receive requests.

Important: This command must be entered multiple times if more than one SBC is present.

Example

The following commands identify three peer SBCs for a single P-CSCF/A-BG service:

```
peer-sbc 200.6.2.3

peer-sbc 200.6.2.10

peer-sbc 200.6.2.11
```

The following command removes the peer SBC with IP address *200.6.2.10* from the P-CSCF/A-BG service:

```
no peer-sbc 200.6.2.10
```

plmn-id

Configures location specific mobile network identifiers used to help translate local emergency and service-related numbers. Default is disabled.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

plmn-id mcc *code* **mnc** *code*

no plmn-id

mcc *code*

Specifies the Mobile Country Code for the mobile access network. *code* must be a three-digit integer from 200 to 999.

mnc *code*

Specifies the Mobile Network Code for the mobile access network. *code* must be a two or three-digit integer from 00 to 999.

no

Removes the access network configuration for this P-CSCF/A-BG service.

Usage

Use this command to help match location specific emergency/service numbers when configuring translations. The **mcc** and **mnc** values are compared against those received in p-access-network-info headers as per 3GPP TS 24.229. If **mnc** is not provided in the criteria only **mcc** is compared.

Example

The following command identifies the mobile network with a MCC of *123* and a MNC of *12*:

```
plmn-id mcc 123 mnc 12
```

reg-preloaded-route

Enables the function to use the preloaded-route-headers received in REGISTER for routing at P-CSCF.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ default | no ] reg-preloaded-route
```

default | no

Disables the ability to use preloaded-route-headers for routing REGISTER.

Usage

Use this command to enable or disable usage of preloaded-route-headers for routing REGISTER.

reg-service-route

Enables the function to use service routes when routing re-registrations.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ no ] reg-service-route
```

no

Disables the ability to use service routes for re-registration.

Usage

Use this command to enable the P-CSCF/A-BG service to use service routes when routing re-registrations.

reliable-prov-resp

Enables/disables the reliability of provisional responses feature.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
reliable-prov-resp { mandatory | optional }

[ no ] reliable-prov-resp
```

mandatory | optional

mandatory: Both inbound and outbound will request reliability.
optional(default): Reliability is imposed by inbound side. Only if inbound call requests reliability will outbound also request reliability.

no

Disables the reliability of provisional responses feature.

Usage

Use this command to enable/disable the reliability of provisional responses feature.

Example

The following command sets the reliability of provisional responses feature to mandatory:

```
reliable-prov-resp mandatory
```

The following command disables the reliability of provisional responses feature:

```
no reliable-prov-resp
```

restoration-procedure

Enables the P-CSCF/A-BG service to reject with a 504 response when it receives 3xx, 480, or “no response” to service request. This feature is disabled by default.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ no ] restoration-procedure
```

no

Disables restoration procedure on the P-CSCF/A-BG service.

Usage

Restoration procedure is intended to handle unreachability of service-route header content. Enabling this command allows the P-CSCF/A-BG service to reject with a 504 response when it receives 3xx, 480, or “no response” to service request.

Example

Enables restoration procedure on the P-CSCF/A-BG service:

```
restoration-procedure
```

Disables restoration procedure on the P-CSCF/A-BG service:

```
no restoration-procedure
```

security-parameters

Enters the Security Configuration Mode in which Denial of Service (DOS) prevention commands can be configured.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
security-parameters
```

Usage

Use this command to enter the Security Configuration Mode.
Entering this command results in the following prompt:

```
[context_name]hostname(config-security-parameters)#
```

Security Configuration Mode commands are defined in the *CSCF Security Configuration Mode Commands* chapter in this guide.

sigcomp

Enables signaling compression for the P-CSCF/A-BG service and enters the Signaling Compression Configuration Mode.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ no ] sigcomp
```

no

Disables signaling compression for the P-CSCF/A-BG service.

Usage

Use this command to enable signaling compression for the P-CSCF/A-BG service and enter the CSCF Signaling Compression Configuration Mode.
Entering this command results in the following prompt:

```
[context_name]hostname(config-sigcomp)#
```

Signaling Compression Configuration Mode commands are defined in the *CSCF Signaling Compression Configuration Mode Commands* chapter in this guide.

sip-header

Enable SIP header insertion for the P-CSCF/A-BG service. SIP header insertion is disabled by default.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ no ] sip-header insert { p-access-network-info | p-cust1-prid-info | p-user-database }
```

no

Disables SIP header insertion for the P-CSCF/A-BG service.

insert { p-access-network-info | p-cust1-prid-info | p-user-database }

p-access-network-info: Inserts P-Access-Network-Info (PANI) header in received request/response.
p-cust1-prid-info: Inserts a custom header, P-LGUPlus-PRID-Info, which contains the private user id of the user sending any dialogue creating request or any standalone requests, to be added in the message toward nexthop. Addition of the header will be done when P-CSCF forwards this message.
p-user-database: Inserts P-User-Database (PUD) header in SIP (REGISTER) message and Invite from I-CSCF to S-CSCF.

Usage

Enabling this command allows SIP header insertion on the P-CSCF or A-BG.

Important: Use the **access-type** command to configure a ue-ip-address-range per access type. CSCF Service Configuration Mode commands are defined in the *CSCF Service Configuration Mode Commands* chapter in this guide.

Example

Enables SIP PANI header insertion for the P-CSCF/A-BG service:

```
sip-header insert p-access-network-info
```

sip-param

Enable the addition of "integrity-protected" parameter in the authorization header of a SIP (REGISTER) message for the P-CSCF/A-BG service.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ no ] sip-param insert integrity-protected [ transparent ]
```

no

Disables the addition of "integrity-protected" parameter in the authorization header of a SIP (REGISTER) message for the P-CSCF/A-BG service.

insert integrity-protected

Inserts "integrity-protected" parameter in the authorization header of a SIP (REGISTER) message for the P-CSCF/A-BG service.

transparent

Pass the "integrity-protected" parameter received from the previous node unmodified.

Usage

Enabling this command allows the P-CSCF or A-BG to add the "integrity-protected" parameter in the authorization header of a SIP (REGISTER) message. The parameter will be used by the S-CSCF to decide which authentication mode to use to authenticate the user.

Example

Enables the addition of **integrity-protected** parameter:

```
sip-param insert integrity-protected
```

Disables the addition of **integrity-protected** parameter:

```
no sip-param insert integrity-protected
```

store-session-path

Enables the P-CSCF or A-BG to store and process the session path information, which includes the Route list, Record-Route list, Service-Route list, and ViaList.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
[ no ] store-session-path
```

no

Disables the storing of session path information by the P-CSCF or A-BG. In addition, the P-CSCF/A-BG will not overwrite the Route list, Record-Route list, Service-Route list, or ViaList in the in-dialog request and responses.

Usage

Enabling this command allows the P-CSCF or A-BG to store and process the session path information.

Example

Enables the storage and processing of session path information:

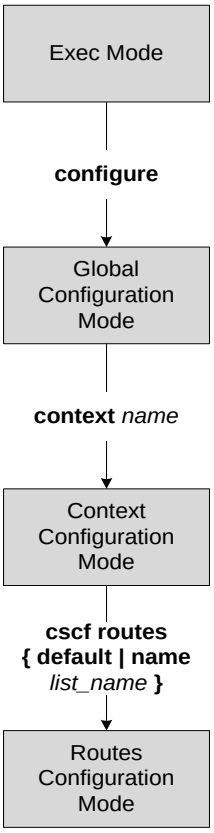
```
store-session-path
```

Disables the storage and processing of session path information:

```
no store-session-path
```

Chapter 86
CSCF Routes Configuration Mode Commands

The CSCF Routes Configuration Mode is used to configure session forwarding within the system.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

after

Places the CSCF route entry at the bottom or end of the route list. Use this command in conjunction with the **route** command.

Product

SCM (P-CSCF, S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

after

Usage

Add this command before the **route** command to place the entry at the end of the route list.

before

Places the CSCF route entry at the top or beginning of the route list. Use this command in conjunction with the **route** command.

Product

SCM (P-CSCF, S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

before

Usage

Add this command before the **route** command to place the entry at the beginning of the route list.

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

exit

Usage

Return to the previous mode.

route

Configure the routing parameters for the context.

Product

SCM (P-CSCF, S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

route { domain *name* **| local { icscf | pcscf | scscf } | nexthop-address** *address* **| peer-servers** *server_name* **| peer-servers-group** *group_name* **| route-list** *group_name* **| vpn** *name* **} [[mod-req-uri] base-criteria** *criteria* **[filter-criteria1** *criteria* **] [filter-criteria2** *criteria* **]] [log]**

no route { domain *name* **| local { icscf | pcscf | scscf } | nexthop-address** *address* **| peer-servers** *server_name* **| peer-servers-group** *group_name* **| route-list** *group_name* **| vpn** *name* **} base-criteria** *criteria* **[filter-criteria1** *criteria* **] [filter-criteria2** *criteria* **]**

domain *name*

Specifies a valid next-hop domain name. *name* must be from 1 to 79 alpha and/or numeric characters in length.

local { icscf | pcscf | scscf }

Specifies a local interrogating, serving, or proxy call/session control function to which all calls processed by the context will be routed.

nexthop-address *ip_address*

Specifies a next-hop address.
ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

peer-servers *server_name*

Specifies a configured peer server.
server_name must be the name of a configured peer server on this system.

peer-servers-group *group_name*

Specifies a configured peer servers group.
group_name must be the name of a configured peer servers group on this system.

route-list *group_name*

Specifies a configured route list group.
group_name must be the name of a configured route list group on this system.

vpn *name*

Specifies a configured VPN context on the system.
name must be a configured context name.

mod-req-uri

Specifies that a route lookup should be performed and the request URI modified.

base-criteria *criteria*

Specifies the base criteria that packets will be compared against. The following criteria is supported:

- **access-type** *type*: Filters sessions based on a specific access-type used by the subscriber. Possible access types are:
  - **3gpp-geran**: 3GPP Access Type
  - **3gpp-utran-fdd**: 3GPP Access Type
  - **3gpp-utran-tdd**: 3GPP Access type
  - **3gpp2-1x**: 3GPP2 Access Type
  - **3gpp2-1x-hrpd**: 3GPP2 Access Type
  - **3gpp2-umb**: 3GPP2-UMB
  - **adsl**: FixedLine Access Type
  - **adsl2**: FixedLine Access Type
  - **adsl2p**: FixedLine Access Type ADSL2+
  - **docsis**: DOCSIS
  - **gshdsl**: Fixed Line Access Type G.SHDSL
  - **hdsl**: Fixed Line Access Type
  - **hdsl2**: Fixed Line Access Type
  - **idsl**: Fixed Line Access Type
  - **ieee-80211**: WLAN Access Type
  - **ieee-80211a**: WLAN Access Type
  - **ieee-80211b**: WLAN Access Type
  - **ieee-80211g**: WLAN Access Type
  - **ieee-80216e**: Wireless MAN Access Type
  - **radsl**: Fixed Line Access Type
  - **sdsl**: Fixed Line Access Type
  - **vdsl**: Fixed Line Access Type
- **any**: Filters all CSCF sessions.
- **carrier-id** *name*: Filters sessions based on the carrier's ID. *name* must be from 1 to 79 alpha and/or numeric characters in length.
- **destination aor** *aor*: Filters sessions based on the destination AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

  Important: The destination aor and carried-id criteria cannot occur in the same route rule.

- **nexthop-uri** *name*: Filters sessions based on Address of Record. *name* must be from 1 to 79 alpha and/or numeric characters in length.

- **plmn-id mcc** *mcc_code* **mnc** *mnc_code*: Filters sessions based on the mobile country and network codes. *mcc_code* must be a three-digit integer from 200 to 999. *mnc_code* must be a two or three-digit integer from 00 to 999.
- **source address** *ip_address*: Filters sessions based on source IP address. *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
- **source aor** *aor*: Filters sessions based on the source AoR. *aor* must be an existing AoR from 1 to 79 characters in length.
- **subscriber-capability** *capability_type*: Filters sessions based on capability of the subscriber. Possible capability types are:
  - **at** - Custom AT Type
  - **audio** - Audio Capability Type
  - **chat** - Custom CHAT Type
  - **cs** - Custom CS Type
  - **ft** - Custom FT Type
  - **im** - Custom IM Type
  - **mms** - Custom MMS Type
  - **msg** - Custom MSG Type
  - **oma-sip-im** - Custom OMA SIP-IM Type
  - **rcs-dp** - Custom RCS-DP Type
  - **rcs-e** - Custom RCS-E Type
  - **rcs-ft** - Custom RCS-FT Type
  - **rcs-im** - Custom RCS-IM Type
  - **rcs-is** - Custom RCS-IS Type
  - **rcs-sp** - Custom RCS-SP Type
  - **rcs-vs** - Custom RCS-VS Type
  - **text** - Text Capability Type
  - **video** - Video Capability Type
  - **vt** - Custom VT Type
  - **vt-ft** - Custom VT-FT Type
  - **vt-is** - Custom VT -IS Type
  - **vt-loc** - Custom VT-LOC Type
  - **vt-memo** - Custom VT-MEMO Type
- **subscriber-ip-type { v4 | v6 }**: Filters sessions based on IP type of the subscriber. Possible IP types are:
  - **v4** - IPV4 Type
  - **v6** - IPV6 Type
- **time-of-day**: Filters sessions based on the time of the day. Additional filter criteria for **time-of-day** is as follows:

- **day-of-month** *day*: Filters session based on the day of the month. *day* must be an integer from 1 to 31.
- **day-of-week** *day*: Filters session based on the day of the week. *day* must be an integer from 1 to 7 with 1 signifying Sunday and 7 signifying Saturday.
- **start** *date/time* **[end** *date/time* **]**: Filters sessions based on a start time to, optionally, an end time during the day. *date/time* must be integers in either of the following formats: YYYY:MM:DD:HH:mm or YYYY:MM:DD:mm:ss. YYYY: year range 2005 to 2099 MM: months (integer range 1 to 12) DD: days (integer range 1 to 31) HH: hours (integer range 0 to 23) mm: minutes (integer range 0 to 59) ss: seconds (integer range 0 to 59)
- **week-of-month** *week*: Filters sessions based on the week of the month. *week* must be an integer from 1 to 5.

Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

filter-criteria1 *criteria*

Specifies the filter criteria that packets that have passed the base criteria will be compared against. The following criteria is supported:

- **access-type** *type*: Filters sessions based on a specific access-type used by the subscriber. Possible access types are:
  - **3gpp-geran**: 3GPP Access Type
  - **3gpp-utran-fdd**: 3GPP Access Type
  - **3gpp-utran-tdd**: 3GPP Access type
  - **3gpp2-1x**: 3GPP2 Access Type
  - **3gpp2-1x-hrpd**: 3GPP2 Access Type
  - **3gpp2-umb**: 3GPP2-UMB
  - **adsl**: FixedLine Access Type
  - **adsl2**: FixedLine Access Type
  - **adsl2p**: FixedLine Access Type ADSL2+
  - **docsis**: DOCSIS
  - **gshdsl**: Fixed Line Access Type G.SHDSL
  - **hdsl**: Fixed Line Access Type
  - **hdsl2**: Fixed Line Access Type
  - **idsl**: Fixed Line Access Type
  - **ieee-80211**: WLAN Access Type
  - **ieee-80211a**: WLAN Access Type
  - **ieee-80211b**: WLAN Access Type
  - **ieee-80211g**: WLAN Access Type
  - **ieee-80216e**: Wireless MAN Access Type
  - **radsl**: Fixed Line Access Type

- **sdsl**: Fixed Line Access Type
- **vdsl**: Fixed Line Access Type

- **any**: Filters all CSCF sessions.
- **carrier-id** *name*: Filters sessions based on the carrier's ID. *name* must be from 1 to 79 alpha and/or numeric characters in length.
- **destination aor** *aor*: Filters sessions based on the destination AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

> ***Important:*** The destination aor and carried-id criteria cannot occur in the same route rule.

- **nexthop-uri** *name*: Filters sessions based on Address of Record. *name* must be from 1 to 79 alpha and/or numeric characters in length.
- **plmn-id mcc** *mcc_code* **mnc** *mnc_code*: Filters sessions based on the mobile country and network codes. *mcc_code* must be a three-digit integer from 200 to 999. *mnc_code* must be a two or three-digit integer from 00 to 999.
- **source address** *ip_address*: Filters sessions based on source IP address. *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
- **source aor** *aor*: Filters sessions based on the source AoR. *aor* must be an existing AoR from 1 to 79 characters in length.
- **subscriber-capability** *capability_type*: Filters sessions based on capability of the subscriber. Possible capability types are:
  - **at** - Custom AT Type
  - **audio** - Audio Capability Type
  - **chat** - Custom CHAT Type
  - **cs** - Custom CS Type
  - **ft** - Custom FT Type
  - **im** - Custom IM Type
  - **mms** - Custom MMS Type
  - **msg** - Custom MSG Type
  - **oma-sip-im** - Custom OMA SIP-IM Type
  - **rcs-dp** - Custom RCS-DP Type
  - **rcs-e** - Custom RCS-E Type
  - **rcs-ft** - Custom RCS-FT Type
  - **rcs-im** - Custom RCS-IM Type
  - **rcs-is** - Custom RCS-IS Type
  - **rcs-sp** - Custom RCS-SP Type
  - **rcs-vs** - Custom RCS-VS Type
  - **text** - Text Capability Type
  - **video** - Video Capability Type

- **vt** - Custom VT Type
- **vt-ft** - Custom VT-FT Type
- **vt-is** - Custom VT -IS Type
- **vt-loc** - Custom VT-LOC Type
- **vt-memo** - Custom VT-MEMO Type

- **subscriber-ip-type { v4 | v6 }**: Filters sessions based on IP type of the subscriber. Possible IP types are:
  - **v4** - IPV4 Type
  - **v6** - IPV6 Type
- **time-of-day**: Filters sessions based on the time of the day. Additional filter criteria for **time-of-day** is as follows:
  - **day-of-month** *day*: Filters session based on the day of the month. *day* must be an integer from 1 to 31.
  - **day-of-week** *day*: Filters session based on the day of the week. *day* must be an integer from 1 to 7 with 1 signifying Sunday and 7 signifying Saturday.
  - **start** *date/time* **[end** *date/time* **]**: Filters sessions based on a start time to, optionally, an end time during the day. *date/time* must be integers in either of the following formats: YYYY:MM:DD:HH:mm or YYYY:MM:DD:mm:ss. YYYY: year range 2005 to 2099 MM: months (integer range 1 to 12) DD: days (integer range 1 to 31) HH: hours (integer range 0 to 23) mm: minutes (integer range 0 to 59) ss: seconds (integer range 0 to 59)
  - **week-of-month** *week*: Filters sessions based on the week of the month. *week* must be an integer from 1 to 5.

Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

filter-criteria2 *criteria*

Specifies the filter criteria that packets that have passed the base criteria and filter-criteria1 will be compared against. The following criteria is supported:

- **access-type** *type*: Filters sessions based on a specific access-type used by the subscriber. Possible access types are:
  - **3gpp-geran**: 3GPP Access Type
  - **3gpp-utran-fdd**: 3GPP Access Type
  - **3gpp-utran-tdd**: 3GPP Access type
  - **3gpp2-1x**: 3GPP2 Access Type
  - **3gpp2-1x-hrpd**: 3GPP2 Access Type
  - **3gpp2-umb**: 3GPP2-UMB
  - **adsl**: FixedLine Access Type
  - **adsl2**: FixedLine Access Type
  - **adsl2p**: FixedLine Access Type ADSL2+
  - **docsis**: DOCSIS

- **gshdsl**: Fixed Line Access Type G.SHDSL
- **hdsl**: Fixed Line Access Type
- **hdsl2**: Fixed Line Access Type
- **idsl**: Fixed Line Access Type
- **ieee-80211**: WLAN Access Type
- **ieee-80211a**: WLAN Access Type
- **ieee-80211b**: WLAN Access Type
- **ieee-80211g**: WLAN Access Type
- **ieee-80216e**: Wireless MAN Access Type
- **radsl**: Fixed Line Access Type
- **sdsl**: Fixed Line Access Type
- **vdsl**: Fixed Line Access Type

- **any**: Filters all CSCF sessions.
- **carrier-id** *name*: Filters sessions based on the carrier's ID. *name* must be from 1 to 79 alpha and/or numeric characters in length.
- **destination aor** *aor*: Filters sessions based on the destination AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

> ***Important:*** The destination aor and carried-id criteria cannot occur in the same route rule.

- **nexthop-uri** *name*: Filters sessions based on Address of Record. *name* must be from 1 to 79 alpha and/or numeric characters in length.
- **plmn-id mcc** *mcc_code* **mnc** *mnc_code*: Filters sessions based on the mobile country and network codes. *mcc_code* must be a three-digit integer from 200 to 999. *mnc_code* must be a two or three-digit integer from 00 to 999.
- **source address** *ip_address*: Filters sessions based on source IP address. *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
- **source aor** *aor*: Filters sessions based on the source AoR. *aor* must be an existing AoR from 1 to 79 characters in length.
- **subscriber-capability** *capability_type*: Filters sessions based on capability of the subscriber. Possible capability types are:
  - **at** - Custom AT Type
  - **audio** - Audio Capability Type
  - **chat** - Custom CHAT Type
  - **cs** - Custom CS Type
  - **ft** - Custom FT Type
  - **im** - Custom IM Type
  - **mms** - Custom MMS Type
  - **msg** - Custom MSG Type

- **oma-sip-im** - Custom OMA SIP-IM Type
- **rcs-dp** - Custom RCS-DP Type
- **rcs-e** - Custom RCS-E Type
- **rcs-ft** - Custom RCS-FT Type
- **rcs-im** - Custom RCS-IM Type
- **rcs-is** - Custom RCS-IS Type
- **rcs-sp** - Custom RCS-SP Type
- **rcs-vs** - Custom RCS-VS Type
- **text** - Text Capability Type
- **video** - Video Capability Type
- **vt** - Custom VT Type
- **vt-ft** - Custom VT-FT Type
- **vt-is** - Custom VT -IS Type
- **vt-loc** - Custom VT-LOC Type
- **vt-memo** - Custom VT-MEMO Type

- **subscriber-ip-type { v4 | v6 }**: Filters sessions based on IP type of the subscriber. Possible IP types are:
  - **v4** - IPV4 Type
  - **v6** - IPV6 Type
- **time-of-day**: Filters sessions based on the time of the day. Additional filter criteria for **time-of-day** is as follows:
  - **day-of-month** *day*: Filters session based on the day of the month. *day* must be an integer from 1 to 31.
  - **day-of-week** *day*: Filters session based on the day of the week. *day* must be an integer from 1 to 7 with 1 signifying Sunday and 7 signifying Saturday.
  - **start** *date/time* **[end** *date/time* **]**: Filters sessions based on a start time to, optionally, an end time during the day. *date/time* must be integers in either of the following formats: YYYY:MM:DD:HH:mm or YYYY:MM:DD:mm:ss. YYYY: year range 2005 to 2099 MM: months (integer range 1 to 12) DD: days (integer range 1 to 31) HH: hours (integer range 0 to 23) mm: minutes (integer range 0 to 59) ss: seconds (integer range 0 to 59)
  - **week-of-month** *week*: Filters sessions based on the week of the month. *week* must be an integer from 1 to 5.

Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

log

Enables logging for CSCF sessions meeting the criteria specified in the ACL. The logs can be viewed by executing the **logging filter active facility cscf-acl-log** command in the Exec mode.

no route { domain *name* **| local { icscf | pcscf | scscf } | nexthop-address** *address* **| peer-servers** *group_name* **| route-list** *group_name* **| vpn** *name* **} base-criteria** *criteria* **[filter-criteria1** *criteria* **] [filter-criteria2** *criteria* **]**

Removes the specified routing parameters for the CSCF service.

Usage

Use this command to configure routing parameters for the service.

Important: Use the **before** or **after** command to place the route entry in the route list.

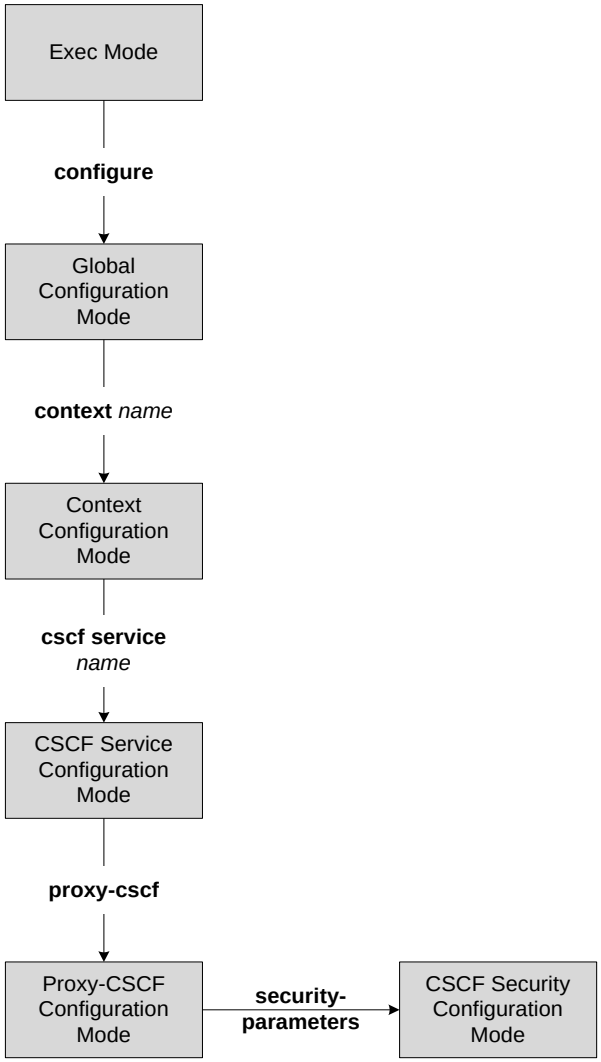
Example

The following command is placed at the end of the route list and routes sessions to a peer server group named *icscf_peer5*, filters sessions with a base criteria of the source address (*1.2.3.4*) and a filter criteria of the destination AoR (*$.@test.com*):

```
after route peer-servers icscf_peer5 base-criteria source address 1.2.3.4
filter-criteria1 destination aor $.@test.com
```

Chapter 87
CSCF Security Configuration Mode Commands

The CSCF Security Configuration Mode is used to configure Denial of Service (DOS) prevention commands.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

auth-failure-weight

Sets a severity number for authorization failures used in calculating a value for determining when to suspend registration attempts.

Important: The system will ignore the configuration of this command unless the **dos-prevention** command has been enabled.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Syntax

auth-failure-weight *weight*

default auth-failure-weight

weight

Default: 1
Assigns a weight to an authorization failure. Defines the severity of a single authorization failure.
weight must be an integer from 1 to 5.

default

Sets /restores the default value assigned to the specified command.

Usage

Use this command to define the severity of an authorization failure. This parameter is used in calculating the current number of authorization failures to compare to the **per-aor-failure-limit** and the **per-ip-failure-limit**. Configuring this command with a lower number causes the system to suspend registration attempts with repeated authorization failures much sooner than when configured with a higher number.

Example

The following command assigns a weight of *3* to an authorization failure:

```
auth-failure-weight 3
```

bad-request-weight

Sets a severity number for bad registration requests used in calculating a value for determining when to suspend registration attempts.

Important: The system will ignore the configuration of this command unless the **dos-prevention** command has been enabled.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Syntax

bad-request-weight *weight*

default bad-request-weight

weight

Default: 2
Assigns a weight to a bad registration request. Defines the severity of a single bad request.
weight must be an integer from 1 to 5.

default

Sets /restores the default value assigned to the specified command.

Usage

Use this command to define the severity of bad registration request. This parameter is used in calculating the current number of request failures to compare to the **per-aor-failure-limit** and the **per-ip-failure-limit**. Configuring this command with a lower number causes the system to suspend registration attempts with repeated request failures much sooner than when configured with a higher number.

Example

The following command assigns a weight of *3* to a bad registration request:

```
bad-request-weight 3
```

dos-prevention

Enables the denial of service prevention feature.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] dos-prevention
```

[default | no]

Disables the denial of service prevention feature.

Usage

Use this command to enable the denial of service prevention feature. The default value for this command is disabled. When this command is enabled, the commands in this mode are enabled with default values configured.

Important: This command must be enabled before configuring other commands in this mode.

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the previous mode.

forking-contact-limit

Sets a limit on the number of contacts a user ID can register with the system.

Important: The system will ignore the configuration of this command unless the **dos-prevention** command has been enabled.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Syntax

forking-contact-limit *limit*

default forking-contact-limit

limit

Default: 0
Sets the maximum number of contacts a user ID can register with the system. 0 specifies that unlimited contacts can be registered per user ID.
limit must be an integer from 0 to 10.

default

Sets /restores the default value assigned to the specified command.

Usage

Use this command to limit the number of contacts a user ID can register with the system.

Example

The following command limits all users to *2* registered contacts on the system:

```
forking-contact-limit 2
```

greylist-duration

Configures the amount of time an AoR or IP address remains on a “grey list” after having crossed the registration authorization limit or the bad registration request limit.

Important: The system will ignore the configuration of this command unless the **dos-prevention** command has been enabled.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Syntax

greylist-duration *time*

default greylist-duration

time

Default: 10
Defines the time, in minutes, that an AoR or IP address remains on a “grey list”.
time must be an integer from 5 to 1,440.

default

Sets /restores the default value assigned to the specified command.

Usage

Use this command to specify the amount of time AoRs or IP addresses remain on a “grey list” after having crossed the registration authorization limit or the bad registration request limit. Limits are described in the **per-aor-failure-limit** command and the **per-ip-failure-limit** command.

Example

The following command sets the duration AoRs or IP addresses remain on a “grey list” to *30* minutes:

```
greylist-duration 30
```

per-aor-failure-limit

Sets a failure limit that, when exceeded, causes the suspension of registration attempts for the offending AoR.

Important: The system will ignore the configuration of this command unless the **dos-prevention** command has been enabled.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Syntax

per-aor-failure-limit *limit*

default per-aor-failure-limit

limit

Default: 200
Defines the threshold for registration failures based on a calculation using weighted multipliers defined in **auth-failure-weight** and **bad-request-weight**.
limit must be an integer from 5 to 10,000.

default

Sets /restores the default value assigned to the specified command.

Usage

Use this command to set a failure limit for registration attempts from an identified AoR. The following calculation determines when this threshold is reached for a specific AoR:
Current authorization failures ÷ **auth-failure-weight** = current failures per AoR
or
Total bad registration requests ÷ **bad-request-weight** = current failures per AoR
If **auth-failure-weight** = *2* and **bad-request-weight** = *1*, and the **per-aor-failure-limit** = *100*, then the tolerance for registration authentication failures = 50 per AoR and the tolerance for bad registration requests = 100 per AoR.
When an AoR reaches the failure limit, it is added to a "grey list" for a period of time as defined by the **greylist-duration** command.

Example

The following command sets the AoR failure limit to *300*:

```
per-aor-failure-limit 300
```

per-ip-failure-limit

Sets a failure limit that, when exceeded, causes the suspension of registration attempts for the offending IP address.

Important: The system will ignore the configuration of this command unless the **dos-prevention** command has been enabled.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Syntax

per-ip-failure-limit *limit*

default per-ip-failure-limit

limit

Default: 100
Defines the threshold for registration failures based on a calculation using weighted multipliers defined in **auth-failure-weight** and **bad-request-weight**.
limit must be an integer from 5 to 10,000.

default

Sets /restores the default value assigned to the specified command.

Usage

Use this command to set a failure limit for registration attempts from an identified IP address. The following calculation determines when this threshold is reached for any IP address:
Current authorization failures ÷ **auth-failure-weight** = current failures per AoR
or
Total bad registration requests ÷ **bad-request-weight** = current failures per AoR
If **auth-failure-weight** = *2* and **bad-request-weight** = *1*, and the **per-ip-failure-limit** = *200*, then the tolerance for registration authentication failures = 100 per each IP address and the tolerance for bad registration requests = 200 per each IP address.
When an IP address reaches the failure limit, it is added to a "grey list" for a period of time as defined by the **greylist-duration** command.

Example

The following command sets the IP address registration failure limit to *200*:

```
per-ip-failure-limit 200
```

threshold-rate

Configures the rate per second at which the system must receive bad requests before it considers the requests a DoS attack.

Important: The system will ignore the configuration of this command unless the **dos-prevention** command has been enabled.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Syntax

threshold-rate *rate*

default threshold-rate

rate

Default: 1
Specifies the rate per second that the system must receive bad requests to determine that it is under a DoS attack.
rate must be an integer from 1 to 1,000.

default

Sets /restores the default value assigned to the specified command.

Usage

Use this command to specify the threshold rate for bad requests. For example, if a malicious user sends bad requests at a rate of 5 per second and this parameter is set to 10, the system will not consider itself under a DoS attack.

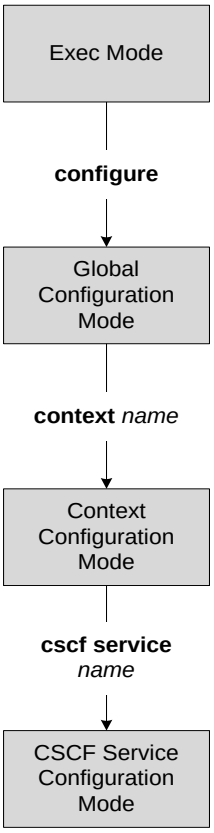
Example

The following command sets the threshold rate to *5* bad requests per second:

```
threshold-rate 5
```

Chapter 88
CSCF Service Configuration Mode Commands

The CSCF Service Configuration Mode is used to create and manage CSCF services within the current context.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

RetryAfter-header-value

Sets the minimum and maximum value in seconds for Retry-After Header.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

RetryAfter-header-value min-value *sec* **max-value** *sec*

default RetryAfter-header-value

min-value *sec* **max-value** *sec*

min-value *sec*: Specifies the minimum amount of time for Retry-After Header. *sec* must be an integer from 2 to 3600. Default is 2 seconds.
max-value *sec*: Specifies the maximum amount of time for Retry-After Header. *sec* must be an integer from 3 to 3601. Default is 10 seconds.

Important: Maximum value should be greater than minimum value.

default

Returns the command to the default settings.

Usage

Use this command to set the minimum and maximum value in seconds for Retry-After Header. If Transactions Per Second (TPS) rate towards the peer-server application server (AS) is exceeded, the incoming requests will be rejected with 500 error response; Retry-After Header specifies the number of seconds before UE should retry.

Example

The following command configures the minimum value to *3*and maximum value to *12* for Retry-After Header:

```
RetryAfter-header-value min-value 3 max-value 12
```

access-service

Configures the name of the P-CSCF/A-BG access service from which the system receives requests and sends responses. The access service lets the core service know where a packet needs to be routed.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
access-service name name
no access-service [ name name ]
```

name *name*

Specifies the name of the P-CSCF/A-BG access service from which the system receives requests and sends responses.
name must be from 1 to 63 alpha and/or numeric characters.

Important: This command should only be issued in the core service configuration, however, multiple access services may be configured per core service.

no

Removes the access service.

Usage

Use this command to identify the name of the P-CSCF/A-BG access service from which the system receives requests and sends responses from/to the UEs. This command is used in systems that deploy two P-CSCF/A-BG services in bridging (Back-to-Back User Agent) mode configurations where an access service P-CSCF/A-BG faces the UE network and a core P-CSCF/A-BG faces the public network.

Example

The following command identifies the P-CSCF/A-BG access service named to the CSCF/A-BG core service:

```
access-service name HA3
```

access-type

Specifies the access types for IMS core.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

access-type { type } access-profile { default | name *access_profile_name* **} | ue-ip-address-range name** *ue_ip_name* **{ address** *ip_address_mask* **| range** *start_ip_address end_ip_address* **}**

no access-type { type } [access-profile | ue-ip-address-range [name *ue_ip_name* **]]**

access-type { type }

3gpp-e-utran-fdd: 3GPP Access Type
3gpp-e-utran-tdd: 3GPP Access Type
3gpp-geran: 3GPP Access Type
3gpp-utran-fdd: 3GPP Access Type
3gpp-utran-tdd: 3GPP Access type
3gpp2-1x: 3GPP2 Access Type
3gpp2-1x-hrpd: 3GPP2 Access Type
3gpp2-umb: 3GPP2-UMB
adsl: FixedLine Access Type
adsl2: FixedLine Access Type
adsl2p: FixedLine Access Type ADSL2+
docsis: DOCSIS
gshdsl: FixedLine Access Type G.SHDSL
hdsl: FixedLine Access Type
hdsl2: FixedLine Access Type
idsl: FixedLine Access Type
ieee-80211: WLAN Access Type
ieee-80211a: WLAN Access Type
ieee-80211b: WLAN Access Type
ieee-80211g: WLAN Access Type
ieee-80211n: WLAN Access Type
ieee-80216e: Wireless MAN Access Type
ieee-8023: Ethernet Access Type
ieee-8023a: Ethernet Access Type
ieee-8023ab: Ethernet Access Type
ieee-8023ae: Ethernet Access Type
ieee-8023ak: Ethernet Access Type
ieee-8023an: Ethernet Access Type
ieee-8023aq: Ethernet Access Type
ieee-8023e: Ethernet Access Type
ieee-8023i: Ethernet Access Type
ieee-8023j: Ethernet Access Type
ieee-8023u: Ethernet Access Type

ieee-8023y: Ethernet Access Type
ieee-8023z: Ethernet Access Type
radsl: FixedLine Access Type
sdsl: FixedLine Access Type
vdsl: FixedLine Access Type

---

access-profile { default | name *access_profile_name* **}**

Associates an access type with a CSCF access profile. Different access types can refer to the same access profile.

---

ue-ip-address-range name *ue_ip_name* **{ address** *ip_address_mask* **| range** *start_ip_address end_ip_address* **}**

Configures UE IP address/range for a specific access type.
ue_ip_name must be from 1 to 79 alpha and/or numeric characters.
address *ip_address_mask*: Specifies a combined IP address subnet mask bits to indicate what IP addresses the specific access-type applies to. *ip_address_mask* must be specified using the form "IP Address/Mask Bits" where the IP address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6, and the mask bits are a numeric value, which is the number of bits in the subnet mask.
range *start_ip_address end_ip_address*: Configure UE IP range for specific access-type.

- *start_ip_address* specifies the beginning of the range of addresses.
- *end_ip_address* specifies the end of the range of addresses.
- *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

---

no

Removes the specified access type from a CSCF access profile or UE IP address/range.

Usage

Use this command to associated the access types for a specified CSCF access profile or UE IP address/range name.

Important: Use the **sip-header** command to enable SIP P-Access-Network-Info (PANI) header insertion. CSCF Proxy-CSCF Configuration Mode commands are defined in the *CSCF Proxy-CSCF Configuration Mode Commands* chapter in this guide.

Example

The following command identifies the access type adsl and assigns it to access profile *ap1*:

```
access-type adsl access-profile name ap1
```

allow-dereg

Allows the CSCF to send de-registration requests. Feature is disabled by default.

Product

SCM

Privilege

Administrator

Syntax

```
[ no ] allow-dereg
```

no

Disables the feature.

Usage

Use this command to allow the CSCF service to send de-registration requests.
If the UE stops sending keepalive packets, which ends the connection between the UE and the proxy, UE information is cleared from the Proxy-CSCF (P-CSCF) or Access Border Gateway (A-BG). If de-registration requests are enabled, any UE-related information that is shared with the Serving-CSCF (S-CSCF) will also be cleared.

bind

Binds the CSCF service to a logical IP interface and specifies the maximum number of sessions that can access this service over the specified interface.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

bind address *ip_address* **[cscf-hostname** *host_name* **] [ipsec-crypto-template** *template* **] [max-sessions** *max#* **] [port** *number* **] [reserved-call-capacity** *percentage* **] [tls-crypto-template** *template* **[tls-port** *number* **]] [transport tcp] [use-serviceport-towards-network]**

no bind address

---

address *ip_address*

Specifies the IP address of the interface to which the service is being bound.
ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

---

cscf-hostname *host_name*

Specifies the local host name of the CSCF service.
host_name must be an existing CSCF service name and be from 1 to 127 alpha and/or numeric characters.
Configuring this keyword associates the CSCF service with the AOR domain configured in the **default-aor-domain** command and uses the domain name in SIP headers.

Important: If this keyword is not configured, SIP headers will contain the IP address of the CSCF service instead of the domain name.

---

ipsec-crypto-template *template*

Specifies the name of an existing IPSec CSCF crypto template to be used for accessing CSCF service by user equipment. Valid only for P-CSCF or A-BG.
template must be an existing IPSec CSCF crypto template and be from 1 to 127 alpha and/or numeric characters.

Important: The IPSec CSCF crypto template should be configured in the same context in which the P-CSCF is configured.

---

max-sessions *max#*

Default: 500,000
Specifies the maximum number of sessions managed by this service on this interface.
max# must be configured to any integer value from 0 to 500,000.

Important: The total session capacity of the system is 500,000. **max-sessions** is also limited by the capacity in the license generated for the service. If licenses for PDSN/GGSN/HA are generated for *x* number of sessions, then the license for the CSCF service will be generated at 500,000-*x*. Hardware configuration and installed features can also affect the maximum number of sessions that can be supported.

port *number*

Default: 5060
Specifies the UDP port number.
number must be an integer value from 1 to 65534.

reserved-call-capacity *percentage*

Default: 10
Specifies the call capacity percentage per session manager (sessmgr).
percentage must be an integer value from 1 to 50.

tls-crypto-template *template* **[tls-port** *number* **]**

Specifies the name of an existing Transport Layer Security (TLS) crypto template to enable TLS functionality. Valid only for P-CSCF or A-BG.
template must be an existing TLS crypto template and be from 1 to 127 alpha and/or numeric characters.
Default: 5061
Specifies the TLS port number.
number must be an integer value from 1 to 65534.

Important: When the **tls-crypto-template** is configured, TCP transport must be enabled, otherwise this command will throw an error. The configured **tls-crypto-template** should be should be configured in the same context in which the P-CSCF service is configured and must be complete with all certificate and cipher suite configuration. If the **tls-crypto-template** is not present or not completely configured, the P-CSCF service will not be started.

transport tcp

Enables TCP transport for the address.

use-serviceport-towards-network

Enables use of service port for sending and receiving UDP messages from network elements.

no

Removes the binding of the service to a specified interface.

Usage

Use this command to associated the service with a specific logical IP address. This command also configures the identity of the CSCF in SIP headers as either the domain name of the CSCF service or the IP address.

Important: Multiple keywords can be used per bind command.

Example

The following command binds the CSCF service to a logical interface with an IP address of *1.2.3.4* and sets the maximum number of supported sessions for this interface at *250000*:

```
bind address 1.2.3.4 max-sessions 250000
```

caller-preference

Enables custom SIP caller preferences; standards-based caller preference will not be applied.

Product

SCM

Privilege

Administrator

Syntax

```
caller-preference custom

[ default | no ] caller-preference
```

default

Enables standards-based caller preference.

no

Disables custom caller preference processing; contact will be selected without considering caller preference.

Usage

Use this command to enable or disable custom SIP caller preferences.

charging

Enables Rf charging in this CSCF service for SIP messages.

Product

SCM

Privilege

Administrator

Syntax

`[ default | no ] charging`

`default | no`

Disables Rf charging in this CSCF service for SIP messages.

Usage

Use this command to enable the RF charging feature in this service and enter the CSCF Charging Configuration Mode.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-charging)#
```

CSCF Charging Configuration Mode commands are defined in the *CSCF Charging Configuration Mode Commands* chapter in this guide.

cnsa-media-profile

Configures the media profile id to be set for a previously created service policy.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
[ no ] cnsa-media-profile profile_id cscf-service-policy policy_name content-type {
application-3gpp-ims-xml | application-pidf-diff-xml | application-pidf-partial-xml |
application-pidf-xml | application-reginfo-xml | application-sdp | application-xml |
message-sipfrag | multipart-mixed | multipart-related | text-plain }
```

---

no

Removes the media profile from the service policy.

---

cnsa-media-profile *profile_id*

Specifies the media profile id.
profile_id must be an integer from 0 to 10 and be an existing media profile id in the system. CNSA media profile ids are created and maintained in the CSCF ISC Template Configuration Mode.

---

cscf-service-policy *policy_name*

Assigns the media profile id to a service policy.
policy_name must be from 1 to 63 alpha and/or numeric characters and be an existing policy name in the system. Service policies are created and maintained in the CSCF Policy Configuration Mode.

---

content-type { application-3gpp-ims-xml | application-pidf-diff-xml | application-pidf-partial-xml | application-pidf-xml | application-reginfo-xml | application-sdp | application-xml | message-sipfrag | multipart-mixed | multipart-related | text-plain }

Specifies the content type(s).
application-3gpp-ims-xml - format for exchanging information in SIP Requests and Responses as used within the 3GPP IM CN Subsystem
application-pidf-diff-xml - contains changed presence elements. Contains full presence document when there are many changes
application-pidf-partial-xml - contains only changed parts of PIDF-based presence information
application-pidf-xml - XML MIME entity that contains presence information
application-reginfo-xml - used in Notifications to SIP user agents about registration expiry
application-sdp - SDP session description
application-xml - content type for generic xml documents
message-sipfrag - contains subsets of well formed SIP messages
multipart-mixed - intended for use when the body parts are independent and need to be bundled in a particular order
multipart-related - intended for compound objects consisting of several inter-related body parts
text-plain - plain text

Important: You may specify multiple types of content.

Usage

Use this command to assign a media profile id to a service policy. The policies defined in the service policy apply to all subscribers using this service.
CNSA media profile ids are created and maintained in the CSCF ISC Template Configuration Mode. Service policies are created and maintained in the CSCF Policy Configuration Mode.

Example

The following command defines the media profile id as *2* and assigns it to *serv_policy3* with plain text content type.

```
cnsa-media-profile 2 cscf-service-policy serv_policy3 content-type text-
plain
```

core-service

Configures a core service if:

- CSCF services are run in bridging (Back-to-Back User Agent) mode
- A-BG is an Application-level Gateway (ALG) for Network Address Translation (NAT)

By default, no core-service name will be present.

Product

SCM (CSCF, A-BG)

Privilege

Administrator

Syntax

[no] core-service name *service_name*

no

Removes the core service.

name *service_name*

Specifies the name of the core service.
service_name must be from 1 to 80 alpha and/or numeric characters.

Usage

Use this command to assign a core service to the CSCF/A-BG service.

Example

The following command identifies the core service:

```
core-service name service1
```

custom reg-binding

Enables the S-CSCF to return only one binding (latest contact) for each registration without including other bindings, if any. Default is disabled.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
[ no ] custom reg-binding
```

no

S-CSCF returns all the bindings for AOR in 200 OK REGISTER response.

Usage

Use this command to control whether the S-CSCF returns only one or all bindings for AOR in 200 OK REGISTER response.

custom response

Configures reject with specific response code for UE capability failure or UE status. Feature is disabled by default.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

custom response { ue-capability-failure *capability_type* **| ue-status** *status* **} reject response-code** *response_code*

no custom response { ue-capability-failure *capability_type* **| ue-status** *status* **}**

ue-capability-failure *capability_type*

Specifies UE capability failure type:

- **all** - UE capability all
- **at** - UE capability AT
- **audio** - UE capability audio
- **chat** - UE capability CHAT
- **cs** - UE capability CS
- **ft** - UE capability FT
- **im** - UE capability IM
- **mms** - UE capability MMS
- **msg** - UE capability MSG
- **oma-sip-im** - UE capability OMA SIP-IM
- **rcs-dp** - UE capability RCS-e DP
- **rcs-e** - UE capability RCS-E
- **rcs-ft** - UE capability RCS-e FT
- **rcs-im** - UE capability RCS-e IM
- **rcs-is** - UE capability RCS-e IS
- **rcs-sp** - UE capability RCS-e SP
- **rcs-vs** - UE capability RCS-e VS
- **text** - UE capability text
- **video** - UE capability video
- **vt** - UE capability VT
- **vt-ft** - UE capability VT-FT
- **vt-is** - UE capability VT-IS
- **vt-loc** - UE capability VT-LOC

- **vt-memo** - UE capability VT-MEMO

ue-status *status*

Specifies UE status:

- **1x-busy** - UE status 1x-busy
- **all** - UE status all
- **idle** - UE status idle
- **power-off** - UE status power-off
- **unreg** - UE status unreg
- **vt-busy** - UE status vt-busy

reject response-code *response_code*

Specifies reject for UE capability failure with specific response code.
response_code must be an integer from 400 to 699.

no

Removes customer-specific UE capability failure or UE status configuration, if present, and uses default RFC/3GPP specification behavior.

Usage

As per RFC/3GPP specifications, S-CSCF rejects with 480 response code for UE capability failure (caller preference) or UE status. Use this command to configure the S-CSCF to reject with specific response code based on UE capability failure or UE status.

Example

The following command configures S-CSCF reject with response code *455* for a UE capability audio failure.

```
custom-response ue-capability-failure audio reject response-code 455
```

custom volte

Enables custom Voice over LTE (VoLTE) features.

Product

SCM

Privilege

Administrator

Syntax

```
[ default | no ] custom volte
```

default | no

Disables custom features.

Usage

Use this command to enable or disable custom VoLTE features.

default-aor-domain

Configures the domain name of the service.

Product

SCM

Privilege

Administrator

Syntax

[no] default-aor-domain *alias*

no

Removes the domain name from the service.

alias

Specifies the domain name for the service.
alias is the name of the domain for this service and must be from 1 to 79 alpha and/or numeric characters in length.

Usage

Use this command to define the domain name of the service.

Example

The following command defines the domain name of the CSCF service as *business.com*:

```
default-aor-domain business.com
```

emergency-cscf

Enables the Emergency-CSCF for the service and enters the Emergency-CSCF Configuration Mode. Default is disabled.

Product

SCM

Privilege

Administrator

Syntax

```
[ no ] emergency-cscf
```

no

Disables the E-CSCF for the service.

Usage

Use this command to enable the Emergency-CSCF feature and enter the Emergency-CSCF Configuration Mode.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-service-emergency-cscf)#
```

Emergency-CSCF Configuration Mode commands are defined in the *CSCF Emergency-CSCF Configuration Mode Commands* chapter in this guide.

Important: Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

```
exit
```

Usage

Return to the previous mode.

history-info

Enables the addition of the history-info header to SIP requests in order to capture request URI information. By default, this command is disabled.

Product

SCM

Privilege

Administrator

Syntax

```
[ default | no ] history-info
```

default | no

Disables the inclusion of the history-info header.

Usage

Use this command to include the history-info header in SIP requests to capture the request URI information for routing or translation.

interface statistics sip

Enables interface SIP statistic collection in this CSCF service.

Product

SCM

Privilege

Administrator

Syntax

```
[ default | no ] interface statistics sip
```

default | no

Disables interface SIP statistic collection for this service.

Usage

Use this command to enable or disable the collection of interface SIP statistics in this service.

interrogating-cscf

This command is not supported in this release.

ipv4-ipv6-interworking

Allows the P-CSCF to provide IPv4-IPv6 interworking when UEs are IPv6-only and the IMS core network is IPv4-only. Feature is disabled by default.

Product

SCM (P-CSCF)

Privilege

Administrator

Syntax

```
[ no ] ipv4-ipv6-interworking
```

no

Disables the feature.

Usage

Use this command to allow IPv4-IPv6 interworking functionality.

keepalive

Configures the CSCF to receive and respond to different types of keep-alive requests.

Product

SCM

Privilege

Administrator

Syntax

```
keepalive [ expire-timer sec [ max-retry num ] | max-retry num [ expire-timer sec ] |
method { crlf | stun } [ expire-timer sec [ max-retry num ] | max-retry num [ expire-
timer sec ] ] ]

default keepalive [ expire-timer | max-retry [ expire-timer ] | method [ expire-timer |
max-retry ] ]

no keepalive [ method { crlf | stun } ]
```

expire-timer *sec*

Default: 29
This value is used according to timed-keepalives parameter present in Path header. UEs are expected to send keepalive messages according to this time interval.
sec must be an integer from 24 to 150.

max-retry *num*

Default: 3
Specifies the maximum number of times the CSCF waits for the UE to send a keepalive request before it deletes the user information.
num must be an integer from 1 to 10.

method { crlf | stun }

Default: both methods enabled.
Specifies the method of keepalive messages supported by the CSCF.
crlf: "\r\n" string (CRLF packets) sent by UE
stun: STUN protocol messages (rfc3489-bis)

default

Returns the command to the default settings. All methods are enabled by default. See keywords above for specific defaults.

no

Disables the specified method of keepalive messages.

Usage

Use this command to configure how the CSCF manages keepalive requests.

Example

The following example sets the expire timer to *40* and the maximum retry parameter to *5*:

```
keepalive expire-timer 40 max-retry 5
```

lawful-intercept

Enables Lawful Intercept (LI) in this CSCF service. Feature is disabled by default.

Product

SCM

Privilege

Administrator

Syntax

```
[ no ] lawful-intercept
```

no

Disables the feature.

Usage

Refer to the *Lawful Intercept Configuration Guide* for more information on LI.

li-packet-cable

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

max-sipmsg-size

Configures the maximum SIP message size.

Product

SCM

Privilege

Administrator

Syntax

max-sipmsg-size *limit*

[default | no] max-sipmsg-size

limit

Default: 4096
Configures the SIP message size limit in bytes.
limit must be an integer from 1024 to 65535.

Important: Maximum SIP message size should be more than the message-max-size set in the CSCF Proxy-CSCF Configuration Mode.

default | no

Returns/sets the maximum SIP message size to 4096 bytes.

Usage

Use this command to configure the maximum SIP message size.

Example

The following command limits the SIP message size to *4500* bytes:

```
max-sipmsg-size 4500
```

media-bridging

Enables SDP modification that terminate media on CSCF. Feature is disabled by default.

Product

SCM (P-CSCF)

Privilege

Administrator

Syntax

media-bridging [v6port-range *start_port end_port* **]**

no media-bridging

v6port-range *start_port end_port*

Specifies port ranges to be used with IPv6 addresses. Only selected ports from the range specified should be used for media bridging.
start_port: Start of port range; must be an integer from 1024 to 65535.
end_port: End of port range; must be an integer from 1025 to 65535.

no

Disables the feature.

Usage

Use this command to allow termination of media on CSCF.

Example

The following command allows media bridging on ports *2000* to *4000* for IPv6 addresses:

```
media-bridging v6port-range 2000 4000
```

monitoring

Enables thresholds alerting for this CSCF service.

Product

SCM

Privilege

Administrator

Syntax

```
monitoring
```

Usage

Use this command to enable thresholds alerting for this CSCF service.

multiple-reg same-private-id

This command allows multiple registrations for the same private user-id from different devices.

Product

SCM (P-CSCF, A-BG, S-CSCF)

Privilege

Administrator

Syntax

```
[ default | no ] multiple-reg same-private-id
```

default | no

Multiple registrations are not allowed for the same private user-id.

Usage

Use this command to allow or disallow multiple registrations for the same private user-id from different devices.

Example

The following command allows multiple registrations for the same private user-id from different devices:

```
multiple-reg same-private-id
```

nat-policy

Configures a NAT (Network Address Translation) policy for the service if the CSCF service is performing one of the following functions:

- CSCF services are run in bridging (Back-to-Back User Agent) mode
- A-BG is an Application-level Gateway (ALG) for NAT

Product

SCM(CSCF, A-BG)

Privilege

Administrator

Syntax

nat-policy *policy_name* { **private-address** { **address** *ip_address_mask* | **default | range** *start_ip_address end_ip_address* } | **bridge-network** { **address** *ip_address_mask* | **range** *start_ip_address end_ip_address* }

no nat-policy *policy_name*

---

policy_name

Specifies a name for the NAT policy.
policy_name must be from 1 to 79 alpha and/or numeric characters.

---

private-address { address *ip_address_mask* **| default|range** *start_ip_address end_ip_address* **}**

Specifies the private-address policy type for nat-pool.
address *ip_address_mask*: Address for nat-policy policy type for nat-pool. Specifies a combined IP address subnet mask bits to indicate what IP addresses the specific policy type applies to. *ip_address_mask* must be specified using the form "IP Address/Mask Bits" where the IP address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6, and the mask bits are a numeric value, which is the number of bits in the subnet mask.
default: Default for nat-policy policy type for nat-pool. Default is defined as the address range specified by rfc1918.

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

range *start_ip_address end_ip_address*: Range for nat-policy policy type for nat-pool.

- *start_ip_address* specifies the beginning of the range of addresses.
- *end_ip_address* specifies the end of the range of addresses .
- *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

---

bridge-network { address *ip_address_mask* **| range** *start_ip_address end_ip_address* **}**

Specifies the bridge-network policy type for S-CSCF bridging.
address *ip_address_mask*: Address for bridge-network policy type for S-CSCF bridging. Specifies a combined IP address subnet mask bits to indicate what IP addresses the specific policy type applies to.

ip_address_mask must be specified using the form "IP Address/Mask Bits" here the IP address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6, and the mask bits are a numeric value, which is the number of bits in the subnet mask.

range *start_ip_address end_ip_address*: Range for bridge-network policy type for S-CSCF bridging.

- *start_ip_address* specifies the beginning of the range of addresses.
- *end_ip_address* specifies the end of the range of addresses.
- *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

no

Removes the specified NAT policy from the service.

Usage

Generally, if a SIP packet has a VIA address (physical address that identifies where the service is located) different from the Source address, ALG functionality is invoked. Even if the VIA and Source addresses are the same, however, this command allows the ALG functionality to be started. For ALG to start, the VIA address should belong to one of the nat-policy address ranges.

Example

The following command identifies the NAT policy named *policy1* with a private-address policy type of *10.10.10.10 255.255.255.0*:

```
nat-policy policy1 private-address address 10.10.10.10 255.255.255.0
```

The following command identifies the NAT policy named *policy2* with a private-address range policy type of *172.162.23.23 172.162.23.230*:

```
nat-policy policy2 private-address address 172.162.23.23 172.162.23.230
```

The following command identifies the NAT policy named *policy3* with a default policy type:

```
nat-policy policy3 private-address default
```

nat-pool

Configures a NAT (Network Address Translation) pool for the service if the CSCF service is performing one of the following functions:

- P-CSCF services are run in bridging (Back-to-Back User Agent) mode
- A-BG is an Application-level Gateway (ALG) for NAT

By default, no nat-pool name will be present.

Product

SCM(P-CSCF, A-BG)

Privilege

Administrator

Syntax

nat-pool name *pool_name* **[signalling-pool** *signalling_pool_name* **]**

no nat-pool name *pool_name*

name *pool_name*

Specifies the name of an existing NAT pool.
pool_name must be from 1 to 32 alpha and/or numeric characters.

Important: NAT pools are created in *Context Configuration Mode* with the **ip pool** command.

signalling-pool *signalling_pool_name*

Specifies the name of an existing IP pool from where IP addresses will be used to fill in signalling headers only.
signalling_pool_name must be from 1 to 32 alpha and/or numeric characters.

Important: If **signalling-pool** is not specified, service IP:port will be filled in signalling headers.

no

Removes the NAT pool from the service.

Usage

Use this command to assign a NAT pool to the P-CSCF/A-BG service.

Example

The following command identifies the NAT pool:

```
nat-pool name pool2
```

policy

Enables or disables early media support and IBCF capability in P-CSCF/A-BG. In addition, configures Interim-Interval value for CSCF accounting sessions, overload response, and the congestion control threshold and tolerance values that are to be monitored on this CSCF service.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

policy { accounting interim-interval *value* **| allow-early-media | ibcf-capability domain** *domain/name* **| overload [drop | redirect** *IPv4_address1* **[weight** *weight1* **] [** *IPv4_address2* **[weight** *weight2* **]] ... | reject] | threshold congestion-control { system-cpu-utilization** *percent* **| tolerance** *percent* **} }**

default policy { allow-early-media | overload | threshold congestion-control { system-cpu-utilization | tolerance } }

no policy { accounting interim-interval | allow-early-media | ibcf-capability domain *domain/name* **| overload [redirect** *IPv4_address1* **] [** *IPv4_address2* **] ... | threshold congestion-control { system-cpu-utilization | tolerance } }**

accounting interim-interval *value*

Default: Disabled
Used to configure Interim-Interval value for CSCF accounting sessions.
value can be configured to any integer value from 50 to 7200. This value is sent in the "Acct-Interim-Interval" AVP of the accounting message. Based on the response message from accounting server, Interim-Interval timer is started.

allow-early-media

Default: Enabled
Allows early media by doing QoS commit during QoS Authorization (with PCRF) in P-CSCF.

ibcf-capability domain *domain/name*

Enables IBCF capability to support Mx reference point in CSCF.
IBCF capability domain name must be entered using from 1 to 80 alpha and/or numeric characters.

Important: This CLI can be repeated to add/delete multiple entities to/from the ibcf-capability domain table. An ibcf-capability domain can be removed by using the **no** keyword; using the **no** keyword without giving any domain name will delete all entries from the list.

overload [drop | redirect *IPv4_address1* **[weight** *weight1* **] [** *IPv4_address2* **[weight** *weight2* **]] ... | reject]**

Configures the overload response for this policy. When the P-CSCF/A-BG becomes congested, this overload policy is used to drop/reject subsequent sessions or redirect them to another server.

drop: Specifies that upon policy overload, the system will drop the session.
redirect: Specifies that upon policy overload, the system will redirect the session to another CSCF.

- *IPv4_address1* must be expressed in dotted decimal notation.
- **weight** *weight1*: Defines the priority of the redirect address.

  weight1 must be an integer from 1 to 10. Default is 1.

reject: Specifies that upon policy overload, the system will reject the session with 503 (Service Unavailable) SIP error response. This is the default setting.

---

threshold congestion-control { system-cpu-utilization *percent* **| tolerance** *percent***}**

Enables congestion control. CSCF performs congestion control based on the memory usage inside every sessmgr at two levels.

- **Level 1**: For every new call/event received, the system checks if sessmgr memory-usage is above a threshold value (such as 95 percent). If it is, memory-congestion is triggered and new call messages are rejected with 500 SIP response. Memory congestion is disabled when memory usage drops by a tolerance value (default is 10 percent).
- **Level 2**: If the sessmgr usage reaches 100 percent, all newly received SIP messages are dropped at the socket layer in that sessmgr except for the BYE message. The new SIP messages are not processed until the memory reaches the threshold value (95 percent).

A trap is also generated whenever sessmgr is in congestion state
system-cpu-utilization *percent*: The average percent utilization of a CPU in a PSC/PSC2/PSC3 running the CSCF service as measured in 10 second intervals.
percent can be configured to any integer value from 0 to 100. This value becomes the upper threshold for triggering the CPU-based congestion for CSCF services. Default is 80
tolerance *percent*: The percentage under a configured threshold that dictates the point at which the condition is cleared.
percent is an integer value from 1 to 25. Default is 5

---

default

Returns the command to the default settings. See keywords above for specific defaults.

---

no

Disables the specified functionality.

Usage

Use this command to set the following policy for this CSCF service:

- Configure Interim-Interval value for CSCF accounting sessions.
- Set QoS support during either the initial SDP response or the 200OK response to the INVITE. When **allow-early-media** is enabled, QoS commit is done during initial SDP answer. When disabled, QoS commit is done during 200OK INVITE. By default, this command is enabled.
- Enable or disable IBCF capability.
- Define the response to an overload condition.
- Set thresholds to dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the CSCF service (congested or clear). The tolerance parameter establishes the threshold at which the condition is cleared.

Important: When congestion is triggered, new CSCF calls are not rejected.

Example

The following command sets the upper threshold for CPU utilization for triggering congestion control at *90%*.

```
policy threshold congestion-control system-cpu-utilization 90
```

The following command sets the tolerance to its default value of *5*.

```
default policy threshold congestion-control tolerance
```

policy-name

Assigns a previously created service policy to this service.

Product

SCM

Privilege

Administrator

Syntax

policy-name *name*

no policy-name

name

Specifies the name of the service policy being assigned to this service.
name must be from 1 to 79 alpha and/or numeric characters and be an existing policy name in the system.
Service policies are created and maintained in the CSCF Policy Configuration Mode.

no

Remove the assigned service policy from this service.

Usage

Use this command to assign a service policy to this service. The policies defined in the service policy apply to all subscribers using this service. Service policies are created and maintained in the CSCF Policy Configuration Mode.

Example

The following command assigns a service policy named *serv_policy3* to this service:

```
policy-name serv_policy3
```

proxy-cscf

Enables the Proxy-CSCF for the service and enters the Proxy-CSCF Configuration Mode. Default is disabled.

Product

SCM (P-CSCF)

Privilege

Administrator

Syntax

```
[ no ] proxy-cscf
```

no

Disables the P-CSCF for the service.

Usage

Use this command to enable the Proxy-CSCF feature and enter the Proxy-CSCF Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-service-proxy-cscf)#
```

Proxy-CSCF Configuration Mode commands are defined in the *CSCF Proxy-CSCF Configuration Mode Commands* chapter in this guide.

Important: The Proxy-CSCF is a license-enabled function of the Session Control Manager. Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.

proxy-serving-cscf

This command is not supported in this release.

recurse-on-redirect-resp

Enables the 3xx recursion feature. If enabled, the service will send further invites to the contacts specified upon receiving a 3xx redirect response. Default is disabled.

Product

SCM

Privilege

Administrator

Syntax

```
[ no ] recurse-on-redirect-resp
```

no

Disables the 3xx recursion feature.

Usage

When enabled and on receipt of a 3xx response, the service will collect the SIP URIs present in the Contact header(s) of 3xx and recursively contact each one of them until the call succeeds. The contacts are tried serially. There is a maximum implementation limit of 50 URIs. Each contact, in turn, can send a 3xx response. The service will honor them and append the new contacts. When disabled, the service treats a 3xx response as the final failure response and declares the call attempt “failed”. By default, this feature is disabled.

Example

Enable recursion on 3xx:

```
recurse-on-redirect-resp
```

Disable recursion on 3xx:

```
no recurse-on-redirect-resp
```

reject-on-cnsa-failure

Enables rejection of messages on Core Network Service Authorization failure. Default is disabled.

Product

SCM

Privilege

Administrator

Syntax

```
[ no ] reject-on-cnsa-failure
```

no

Disables the rejection of messages on Core Network Service Authorization failure.

Usage

Enables rejection of messages on Core Network Service Authorization failure. By default, this feature is disabled.
In a mobile originating case, S-CSCF checks for the presence of P-Preferred-Service (PPS) header. If the header is present, media profile authentication is successful and if the incoming ICSI (IMS Communication Service Identifier) value also matches with one of the values in the service_id list, then the request will be forwarded after replacing the PPS header with PAS (P-Asserted-Service). If media profile authentication fails, S-CSCF will check reject-on-cnsa-failure. If enabled, then call is rejected with 403 message. If disabled, a default ICSI is selected from the service_id list and will be put into PAS while forwarding the request by the S-CSCF on service authentication failure.
In PPS is not received by the S-CSCF and media profile authentication is successful, an ICSI from the service_id list, if present, is selected and will be added in PAS header. If media profile authentication fails, reject-on-cnsa-failure is checked. If enabled, call is rejected with 403 message. If disabled, PAS header is added if service_id list is present with an ICSI value.

Example

Enable rejection of messages on Core Network Service Authorization failure:

```
reject-on-cnsa-failure
```

Disable rejection of messages on Core Network Service Authorization failure:

```
no reject-on-cnsa-failure
```

release-call-on-media-loss

Release call on detection of media loss.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

release-call-on-media-loss media-type audio [timeout *seconds* **]**

no release-call-on-media-loss

media-type audio

Enables the release of SIP calls upon the detection of media loss on media-type audio.

timeout *seconds*

Specifies the media loss timeout value; media loss after timeout value results in call release.
seconds must be an integer from 5 to 3600.
If timeout value is not configured, media loss after 5 seconds results in call release.

no

Disables the release of SIP calls upon the detection of media loss.

Usage

Use this command to enable the release of SIP calls upon the detection of media loss.

Example

Enables the release of SIP calls upon the detection of media loss:

```
release-call-on-media-loss media-type audio
```

Enables the release of SIP calls upon the detection of media loss:

```
no release-call-on-media-loss
```

rfc3261-proxy

Enables RFC3261 proxy (SIP Proxy) for this service and enters the SIP Proxy Configuration Mode. Default is disabled.

Product

SCM (SIP Proxy)

Privilege

Administrator

Syntax

`[ default | no ] rfc3261-proxy`

`default | no`

Disables RFC3261 proxy in this service.

Usage

Use this command to enable the Sip Proxy feature and enter the SIP Proxy Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-service-rfc3261-proxy)#
```

SIP Proxy Configuration Mode commands are defined in the *CSCF SIP Proxy Configuration Mode Commands* chapter in this guide.

Important: The SIP Proxy is a license-enabled function of the Session Control Manager. Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.

serving-cscf

Enables Serving-CSCF for the service and enters the Serving-CSCF Command Mode. Default is disabled.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
[ no ] serving-cscf
```

no

Disables S-CSCF for the service.

Usage

Use this command to enable the Serving-CSCF feature and enter the Serving-CSCF Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-service-serving-cscf)#
```

Serving-CSCF Configuration Mode commands are defined in the *CSCF Serving-CSCF Configuration Mode Commands* chapter in this guide.

Important: The Serving-CSCF is a license-enabled function of the Session Control Manager. Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.

serving-cscf-list

Configure a list of Serving CSCFs and their capabilities.

Product

SCM

Privilege

Administrator

Syntax

```
[ no ] serving-cscf-list server { address address | domain domain } { capability value |
port num { capability value } }
```

no

Removes an entry from this list.

server { address *address* **| domain** *domain* **}**

Specifies the S-CSCF server.
address *address*: IP addresses must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
domain *domain*: Domain names must be entered using from 1 to 80 alpha and/or numeric characters.

capability *value*

Specifies the capability of the S-CSCF server. *value* is assigned by the Service Provider and may be an integer from 1 to 999999.

port *num*

Specifies the port at which service is provided by the S-CSCF server. *num* may be an integer from 1 to 65535.

Usage

Use this command to configure a list of Serving CSCFs and their capabilities.

Important: This command can be entered multiple times to identify multiple Serving CSCFs.

Example

The following command adds a S-CSCF with an IP address of *1.2.3.4* and a capability value of *75* to this service's list:

```
serving-cscf-list server address 1.2.3.4 capability 75
```

session-timer

Configures the session expiry for sessions (Session will expire at the configured value unless refreshed.) and the minimum number of seconds in a session timer (session-expires) value the system will allow.

Product

SCM

Privilege

Administrator

Syntax

session-timer { min-se *sec* **[session-expires** *sec* **] | session-expires** *sec* **[min-se** *sec* **] }**

default session-timer [min-se] [session-expires]

no session-timer

min-se *sec*

Default: 90
Specifies the minimum number of seconds the system will allow a session-expires value in a session request.
sec must be an integer value between 90 and the value of the **session-expires** command.

session-expires *sec*

Default: 1800 (30 minutes)
Specifies the number of seconds a session is allowed exist before it expires.
sec must be an integer value between 90 and 18000.

default

Returns the command to the default settings.

no

Disables the session timer.

Usage

Use this command to set a session expiry value for all invites generated by the SCM and a minimum value for a session request session timer the system will allow. If a session is requested with a timer of less than this command's value, the system will reject the request with a "422 Session Interval Too Small" response code.

Example

The following command sets the session expiry for all sessions generated by the SCM to 60 minutes:

```
session-timer session-expires 3600
```

strict-check configured-aor-domain

Enables strict checking on default-aor-domain so S-CSCF will reject registration and invite if there is a mismatch between AoR in To/From and the configured default-aor-domain.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
[ default | no ] strict-check configured-aor-domain
```

default | no

Disables strict checking on default-aor-domain. This is the default behavior.

Usage

Use this command to enable or disable strict checking on default-aor-domain. This allows support for registration of subscribers from multiple domains.

strict-outbound

When enabled, the CSCF rejects registration without outbound parameters from an already registered AoR (the AoR would have included outbound parameters in a previous registration). When disabled, the CSCF allows registration without outbound parameters from the previously registered AoR.

Product

SCM

Privilege

Administrator

Syntax

```
[ no ] strict-outbound
```

no

Disables the feature. This is the default behavior.

Usage

Use this command to reject registration from a previously registered AoR if the AoR fails to register with outbound parameters but included them in the previous registration.

subscriber-policy-override

Configures the system to allow the subscriber-based policy to override the service-based policy. Default is disabled.

Product

SCM

Privilege

Administrator

Syntax

```
[ default | no ] subscriber-policy-override
```

default | no

Removes the subscriber policy override from the service.

Usage

By default, if a conflict occurs between the subscriber-based policy and the service-based policy, the service policy takes precedence. Use this command to override the default behavior of the system and allow the subscriber-based policy to overrule the service policy.

subscription

Enables the registration event package for the service and configures a system-wide subscription lifetime for all subscribers to the service.

Product

SCM

Privilege

Administrator

Syntax

subscription package reg [lifetime { default *sec* **| max** *sec* **[default** *sec* **] | min** *sec* **[max** *sec* **] [default** *sec* **] }]**

[default | no] subscription package reg

package reg [lifetime { default *sec* **| max** *sec* **] | min** *sec* **}**

default *sec*: Specifies the default amount of time that a subscription can exist on the system. *sec* must be an integer from 60 to max sec -1.
Default: 3761

Important: **default** *sec* must be < or = to max sec and > or = to min sec.

The following keywords are specific to the S-CSCF functionality:
max *sec*: Specifies the maximum amount of time that a subscription can exist on the system.
sec must be an integer from 60 to 2147483646.
Default: 86400

Important: **max** *sec* must be > or = to min sec.

min *sec*: Specifies the minimum amount of time that a subscription can exist on the system.
sec must be an integer from 60 to max sec -1.
Default: 60

Important: **min** *sec* must be < or = to max sec.

default

Returns the command to the default settings.

no

Disables the registration event package for the service.

Usage

Use this command to enable the registration event package for the service and control the amount of time subscriptions are allowed to exist on this service.
The system responds to subscriptions in the following manner:
Using default values:

- If a subscription with an expiration value lower than the service's minimum (60) is received, the service will respond with a 423 Interval Too Small message.
- If a subscription with an expiration value higher than the service's maximum (2147483646) is received, the service will automatically reduce the expiration value to the default value.

If a subscription is received missing the "Expires" value, or the value is malformed, the service will automatically respond with 3761 in the 200OK message.

Example

The following command configures the maximum subscription lifetime to *43200* (12 hours):

```
subscription package reg lifetime max 43200
```

support-content-type any

Validates Content-Type in this CSCF service.

Product

SCM

Privilege

Administrator

Syntax

```
[ no ] support-content-type any
```

no

Disables the feature. If disabled, CSCF service rejects unsupported Content-Type with “415 Unsupported Media Type”.

Usage

Use this command to either allow any type of Content-Type or reject unsupported Content-Type.

Example

Allows any type of Content-Type for the CSCF service:

```
support-content-type any
```

Rejects unsupported Content-Type for the CSCF service:

```
no support-content-type any
```

tcp-proxy

Enables SIP TCP proxy for the CSCF service.

Product

SCM

Privilege

Administrator

Syntax

tcp-proxy [port *port_number* **]**

no tcp-proxy

port *port_number*

Default: 5062
Specifies the port used for SIP TCP proxy connections.
port_number must be an integer from 1 to 65534.

no

Disables SIP TCP proxy for the CSCF service

Usage

Use this command to enable SIP TCP proxy for the CSCF service.

Example

Enables SIP TCP proxy for the CSCF service on port *5062*:

```
tcp-proxy port5062
```

Disables SIP TCP proxy for the CSCF service:

```
no tcp-proxy
```

threshold

Enables thresholds alerting and configuration of thresholds for CSCF Service.

Product

SCM

Privilege

Administrator

Syntax

```
threshold { { call-setup-failures | call-total-active | error-no-resource | error-
presence | error-reg-auth | error-tcp | invite-rcvd-rate | monitoring | reg-rcvd-rate |
reg-total-active | route-failures } high_thresh [ clear low_thresh ] | monitoring }

[ default | no ] threshold monitoring
```

{ call-setup-failures | call-total-active | error-no-resource | error-presence | error-reg-auth | error-tcp | invite-rcvd-rate | reg-rcvd-rate | reg-total-active | route-failures } *high_thresh* **clear** *low_thresh*

call-setup-failures: Number of CSCF call setup failures.
Default: 0
call-total-active: Number of total active CSCF calls.
Default: 0
error-no-resource: Number of CSCF call setup failures due to no-resource.
Default: 0
error-presence: Number of CSCF Presence errors.
Default: 0
error-reg-auth: Number of CSCF Registration Authentication failures.
Default: 0
error-tcp: Number of CSCF call setup failures due to TCP error.
Default: 0
invite-rcvd-rate: Number of CSCF calls per polling interval.
Default: 0
reg-rcvd-rate: Number of CSCF registrations per polling interval.
Default: 0
reg-total-active: Number of total CSCF active registrations.
Default: 0
route-failures: Maximum number of route-failures, after which the alarm/alert will be raised. Default: 5
high_thresh: The high threshold number that must be met or exceeded within the polling interval to generate an alert or alarm. Can be configured to any integer value between 0 and 2000000 (0 and 60000 for route-failures).
clear *low_thresh*: The low threshold number that must be met or exceeded within the polling interval to clear an alert or alarm. Can be configured to any integer value between 0 and 2000000 (0 and 60000 for route-failures).

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

monitoring

Enables thresholds alerting for CSCF Service.

default

Returns the command to the default settings.

no

Disables thresholds alerting for CSCF Service.

Usage

Use this command to:

- enable/disable thresholds alerting for CSCF Service
- set an alert or an alarm when a threshold exceeds the configured level

Alerts or alarms are triggered for the number of registration reply errors on the following rules:

- Enter condition: Actual number > High Threshold
- Clear condition: Actual number < Low Threshold

Example

The following command configures a route failures threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold route-failures 1000 clear 500
```

timeout

Sets timeout values for CSCF and SIP transactions.

Product

SCM

Privilege

Administrator

Syntax

```
timeout { hss-wait sec | map-slr-response sec | no-answer sec | policy-interface sec |
sip { 3gpp-d sec | 3gpp-t1 msec | 3gpp-t2 sec | 3gpp-t4 sec | c sec | d sec | idle-tcp-
connection msec  [ cleanup-timer msec ] | invite-expiry sec | t1 msec | t2 sec | t4 sec }
}

default timeout { hss-wait | map-slr-response | no-answer | policy-interface | sip {
3gpp-d | 3gpp-t1 | 3gpp-t2 | 3gpp-t4 | c | d | idle-tcp-connection | invite-expiry | t1 |
t2 | t4 } }
```

hss-wait *sec*

Default: 5
This timer is used by S-CSCF with HSS interface for timeout.
sec must be an integer from 0 to 2147483646.

map-slr-response *sec*

Default: 15
This timer is used by the E-CSCF for MAP SLR response timeout.
sec must be an integer from 15 to 30.

no-answer *sec*

Default: 100
This timer is specially used for No-Answer Call Feature executed by S-CSCF. The timer will be started as soon as 180 Ringing response is received and No-Answer call feature is enabled. The value of this timer should be always less than INVITE Timeout used by DC-SIP.
sec must be an integer from 0 to 2147483646.

policy-interface *sec*

Default: 5
This timer is used by the P-CSCF/A-BG with Policy interface for timeout.
sec must be an integer from 0 to 2147483646.

sip { 3gpp-d *sec* **| 3gpp-t1** *msec* **| 3gpp-t2** *sec* **| 3gpp-t4** *sec* **| c** *sec* **| d** *sec* **| idle-tcp-connection** *msec* **[cleanup-timer** *msec* **] | invite-expiry** *sec* **| t1** *msec* **| t2** *sec* **| t4** *sec* **}**

Sets transaction and expiry timers for SIP.

- **3gpp-d** *sec*: This timer is used to control the retransmission of 200OK messages to INVITEs after an ACK is sent. The ACK transaction is cleared after this period. This timer is applicable only for unreliable transport. *sec* must be an integer from 0 to 2147483646.

Default: 64*T1 (128 seconds, recommended minimum)

- **3gpp-t1** *msec*: This timer is used to control the time interval between each retransmission. The interval doubles after each retransmission. This is used by P-CSCF/A-BG only when it sending message toward the UE. Example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable transport. *msec* must be an integer from 0 to 4294967294.

  Default: 2000 ms (2 secs, recommended minimum).

- **3gpp-t2** *sec*: This timer is used to control the period for which the request continues to get retransmitted. This is used by P-CSCF/A-BG only when it sending message toward the UE. This timer is applicable both for reliable and unreliable transport. *sec* must be an integer from 0 to 2147483646.

  Default: 16 seconds (recommended minimum).

- **3gpp-t4** *sec*: This timer is used to control the period for which the final response to non-invite transaction should be buffered. The buffered response for the retransmitted non-invite request should be sent within that interval. This timer is applicable only for unreliable transport. *sec* must be an integer from 0 to 2147483646.

  Default: 17 seconds (recommended minimum).

- **c** *sec*: This timer is used for an INVITE transaction; if the response is a provisional response with status codes 101 to 199 inclusive (anything but 100), the proxy must reset timer C for that client transaction. The timer may be reset to a different value, but this value must be greater than 3 minutes (180 seconds). When timer C in S-CSCF fires first, S-CSCF will send CANCEL request to Terminating P-CSCF and Terminating P-CSCF will send CANCEL request to UAS . *sec* must be an integer from 180 to 2147483646.

  Default: 180 seconds

- **d** *sec*: This timer is used to control the retransmission of 200OK to INVITE after ACK is sent. The ACK transaction will be cleared after this interval. This timer is applicable only for unreliable transport. *sec* must be an integer from 0 to 2147483646.

  Default: 64*T1 (32 seconds, recommended minimum)

- **idle-tcp-connection** *msec*: This timer is used for closing idle TCP connections. If there is not activity in the TCP connection for the configuration duration, then the connection will be closed. *msec* must be an integer from 1000 (recommended minimum) to 4294967294.

  Default: 42000 milliseconds.

- **cleanup-timer** *msec*: This timer is used to control how often to check for idle TCP connections. *msec* must be an integer from 2000 to 2147483646.

  Default: 2000 milliseconds.

- **invite-expiry** *sec*: This timer is used by SIP while acting as UA Role and no final response is received for the INVITE request sent. This timer is applicable for both reliable and unreliable transport. *sec* must be an integer from 0 to 2147483646.

  Default: 100 seconds (recommended minimum).

- **t1** *msec*: Specifies the time interval (in microseconds) between each retransmission. The interval doubles after each retransmission, for example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable transport. *msec* must be an integer from 0 to 2147483646.

  Default: 500 milliseconds (recommended minimum).

- **t2** *sec*: This timer is used to control the period for which the request keeps getting retransmitted. This timer is applicable both for reliable and unreliable transport. *sec* must be an integer from 0 to 2147483646. The recommended minimum value for this parameter is 4 seconds.

  Default: 64*T1 (32 seconds)

- **t4** *sec*: This timer is used to control the period for which the final response to non-invite transaction should be buffered so as to send the buffered response for the retransmitted non-invite request within that interval. This timer is applicable only for unreliable transport. *sec* must be an integer from 0 to 2147483646.

  Default: 5 seconds (recommended minimum).

default

Returns the command to the default settings. See keywords above for specific defaults.

Usage

Use this command to configure SIP Stack timers and CSCF service specific timers.

Example

The following command sets the SIP d timer to *64* seconds:

```
timeout sip d 64
```

transport-switching

Sets the message size that triggers a transport protocol switch.

Product

SCM

Privilege

Administrator

Syntax

transport-switching policy protocol tcp trigger msg-size *size*

default transport-switching policy protocol tcp trigger msg-size

policy protocol tcp trigger msg-size *size*

Default: 1300
Specifies the size of the SIP message beyond which transport changes to TCP.
size can be configured to any integer value between 1300 and 65535.

default

Returns the size of the SIP message beyond which transport changes to TCP to 1300 bytes.

Usage

Use this command to configure the size of the SIP message beyond which transport changes to TCP.

Example

Switch to TCP transport protocol when the SIP message size is *4000* bytes or more:

```
transport-switching policy protocol tcp trigger msg-size 4000
```

trusted-domain-entity

Adds trusted network nodes (or entities) to a table used by this service to identify those nodes that can be trusted with subscriber information.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

trusted-domain-entity *address* **[foreign-network] [private-network]**

no trusted-domain-entity *address*

trusted-domain-entity *address*

Specifies the IP address of the network node identified as a trusted entity by this service. *address* must be either an IP address or a domain name. IP addresses must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6. Domain names must be entered using from 1 to 80 alpha and/or numeric characters.

foreign-network

Entity belongs to Foreign Network.

private-network

Entity belongs to Private Network.

no

Removes an entry from this service's trusted domain table.

Usage

Use this command to identify to the service the network entities that can be trusted with subscriber information by this service.

Important: This command can be entered multiple times to identify multiple trusted network entities.

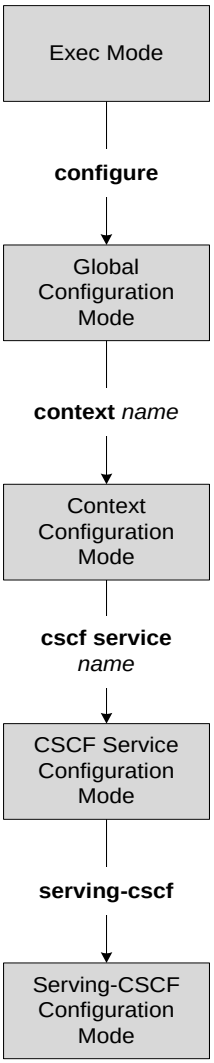
Example

The following command adds a network node with an IP address of *1.2.3.4* to this service's trusted domain table:

```
trusted-domain-entity 1.2.3.4
```

Chapter 89
CSCF Serving-CSCF Configuration Mode Commands

The Serving-CSCF Configuration Mode is used to set various commands supporting the role of the CSCF service as a Serving CSCF.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

3gpp

Enables/disables functionality related to 3GPP Release 8 support. This command is disabled by default.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

3gpp Rel8 Cx { alias-indication | dynamic-password-change | ims-restoration | num-auth-vectors *value* **}**

[default | no] 3gpp Rel8 Cx { alias-indication | dynamic-password-change | ims-restoration | num-auth-vectors }

Rel8 Cx

Specifies functionality related to 3GPP Release 8 support.

alias-indication

Enables alias indication functionality, a collaborative information exchange between the S-CSCF and HSS. Use this command to display alias information from the HSS.
If both the HSS and the S-CSCF support this feature, Alias Group IDs will be displayed in the output of the **show subscribers cscf-only full** command.

dynamic-password-change

Enables dynamic password change support on the S-CSCF service, as per 3GPP 33.203 release 8 version 8.8.0.

ims-restoration

Enables IMS restoration procedures on the S-CSCF service. Use this command to enable IMS REGISTER and INVITE restoration procedures defined in 3GPP TS 23.820.

num-auth-vectors *value*

Enables configurable value for SIP-Number-Auth-Items in MAR.
value must be an integer from 1 to 3. Default is 1.
SCSCF can retrieve multiple authentication vectors from HSS by setting SIP-Number-Auth-Items to an appropriate value. Previously, S-CSCF always set this value to “1”. Using higher values helps to reduce MAR-MAA transactions.

default | no

Disables specified 3GPP Release 8 support feature.

Usage

Use this command to configure the S-CSCF to support 3GPP Release 8 functionality.

Example

The following command enables 3GPP Release 8 alias indication functionality on this service:

```
3gpp Rel8 Cx alias-indication
```

The following command disables 3GPP Release 8 dynamic password change support on this service:

```
no 3gpp Rel8 Cx dynamic-password-change
```

allow rfc3261-ua-interworking

Enables the function to allow IMS interworking with RFC3261 SIP User Agents.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
[ no ] allow rfc3261-ua-interworking
```

no

Disables the interworking capability.

Usage

Use this command to enable the S-CSCF to allow IMS interworking with RFC3261 SIP User Agents.

as-call invite-request-uri update

Enabling this command causes request-URIs in INVITE messages to be updated with the result of the translation before being passed to an Application Server (AS). This command is disabled by default.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

```
[ default | no ] as-call invite-request-uri update
```

default | no

The translation result is ignored.

Usage

Use this command to update the request-URI in INVITE messages with the result of the translation before passing it to an AS.

authentication

Configures the authentication method used by the S-CSCF service.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

```
authentication { aka-v1 value | allow-auth-rsp-failure re-register | allow-hss-failure
re-register | allow-noauth [ invite | re-register| register ] | allow-noipauth [ invite |
re-register| register ] | allow-skip-sar re-register | allow-unsecure | aor-auth |
custom-md5 value | md5 value }

no authentication { aka-v1 | allow-auth-rsp-failure re-register | allow-hss-failure re-
register | allow-noauth [ invite | re-register| register ] | allow-noipauth [ invite |
re-register| register ] | allow-skip-sar re-register | allow-unsecure | aor-auth |
custom-md5 | md5 }
```

aka-v1 *value*

Specifies that AKA-v1 algorithm is used as the authentication type when accessing the CSCF service. *value* specifies a preference - the lower the value, the higher the preference. *value* must be an integer from 1 to 1000.

Important: In order to change a priority level, you must remove the original value and configure a new one.

allow-auth-rsp-failure re-register

Specifies that S-CSCF will not validate authorization received from UE for challenge re-register. If enabled, S-CSCF will send SAR without validating authentication; after receiving SAA, it will send 200 OK for register.

allow-hss-failure re-register

Specifies that S-CSCF should send 200 OK for re-register in case of HSS failure.
When S-CSCF receives register, it sends MAR/SAR to HSS to authenticate the user when authentication is enabled and to get the subscriber profile. When S-CSCF fails to receive response MAA/SAA from HSS, it sends 500 error response to UE. When **allow-hss-failure** is enabled, S-CSCF sends 200 OK for register instead of 500 response.

allow-noauth [invite | re-register| register]

Specifies that access to the S-CSCF service is allowed if authentication fails.
invite: Specifies that access to the S-CSCF service is allowed if authentication fails on INVITE requests only.
re-register: Specifies that access to the S-CSCF service is allowed if authentication fails on RE-REGISTER requests when the request is integrity-protected only.

registration: Specifies that access to the S-CSCF service is allowed if authentication fails on REGISTER requests only.

---

allow-noipauth [invite | re-register| register]

Specifies that access to the S-CSCF service is allowed if early IMS-based IP authentication fails.
invite: Specifies that access to the S-CSCF service is allowed if early IMS-based IP authentication fails on INVITE requests only.
re-register: Specifies that access to the S-CSCF service is allowed if authentication fails on RE-REGISTER requests when the request is integrity-protected only.
registration: Specifies that access to the S-CSCF service is allowed if early IMS-based IP authentication fails on REGISTER requests only.

---

allow-skip-sar re-register

Specifies that S-CSCF should skip SAR to HSS for re-register.
When S-CSCF receives re-register/challenge for re-register, it sends SAR to HSS to get subscriber profile. To avoid overloading HSS, enabling **allow-skip-sar** allows S-CSCF to skip SAR for re-register.

---

allow-unsecure

Specifies that un-secure access is allowed to the S-CSCF service.

---

aor-auth

Specifies that authentication is based on the AoR when accessing the S-CSCF service.

---

custom-md5 *value*

Specifies that custom algorithm HTTP-Digest-MD5 is used as the authentication type for accessing the S-CSCF service. *value* specifies a preference - the lower the value, the higher the preference. *value* must be an integer from 1 to 1000.

Important: In order to change a priority level, you must remove the original value and configure a new one.

---

md5 *value*

Specifies that the MD5 algorithm is used as the authentication type for accessing the S-CSCF service. *value* specifies a preference - the lower the value, the higher the preference. *value* must be an integer from 1 to 1000.

Important: In order to change a priority level, you must remove the original value and configure a new one.

---

no authentication { aka-v1 | allow-auth-rsp-failure re-register | allow-hss-failure re-register | allow-noauth [invite | re-register| register] | allow-noipauth [invite | re-register| register] | allow-skip-sar re-register | allow-unsecure | aor-auth | custom-md5 | md5 }

Disables the specified authentication method for the S-CSCF service.

Usage

Use this command to configure the authentication method used by the S-CSCF service.

Important: The S-CSCF supports multiple authorization schemes, but this requires disabling all authorization configured in the S-CSCF service so that it will send "Unknown" in the Sip-Authorization-Scheme AVP. This allows the HSS to dictate authorization. The following commands disable all authorization configured in the S-CSCF service to allow HSS to control authorization:

```
authentication allow-noipauth

allow rfc3261-ua-interworking

no authentication aka-v1

no authentication md5
```

Example

The following command configures the authentication method used by the S-CSCF service to MD5 with a preference of *3*:

```
authentication md5 3
```

bgcf-proxy

Enables SIP BGCF proxy for the service.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
bgcf-proxy [ port value | transport { tcp | udp } port value ] ]

[ default | no ] bgcf-proxy
```

port *value*

Configures port value for SIP BGCF proxy.
value must be an integer from 1 to 65534.

transport

Enables the specific transport protocol for BGCF proxy.

- **tcp**: Enables TCP transport protocol for BGCF proxy.
- **udp**: Enables UDP transport protocol for BGCF proxy.

default | no

Disables SIP BGCF proxy for the service.

Usage

Use this command to enable or disable SIP BGCF proxy for the service.

Example

The following command enables a SIP BGCF proxy on port *561* for this service:

```
bgcf-proxy port 561
```

The following command disables SIP BGCF proxy for this service:

```
no bgcf-proxy
```

diversion-info

Enabling this command prompts the service to add a diversion header (draft-levy-sip-diversion-08) when the call is diverted to a different endpoint due to a call feature. By default, diversion-info is disabled.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

```
[ default | no ] diversion-info
```

default | no

The service will not add a diversion header.

Usage

Use this command to enable the service to add a diversion header to call setup packets when calls are diverted due to the application of call features.

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

```
exit
```

Usage

Return to the previous mode.

forking

Controls the default-request forking-type in S-CSCF.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
forking { parallel | serial }

[ default | no ] forking
```

parallel | serial

Defines the fork type for request forking.

- **parallel**: Perform parallel forking of request.
- **serial**: Perform serial forking of request.

default

Perform parallel forking of request.

no

Do not perform any forking of request.

Usage

Use this command to control the default-request forking-type in S-CSCF. This configuration will be effective in the absence of "Request-Disposition" header in the message.

Example

The following command enables serial forking of request:

```
forking serial
```

The following command disables any forking of request:

```
no forking
```

interrogating-cscf-role

Enables the function to also perform as an Interrogating-CSCF.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
[ no ] interrogating-cscf-role
```

no

Disables the Interrogating-CSCF role in this function.

Usage

Use this command to enable the S-CSCF to also perform as an Interrogating-CSCF.

local-call-features

Enables/disables local call features. This command is disabled by default.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
[ default | no ] local-call-features
```

default | no

Disables local call features for this S-CSCF.

Usage

Use this command to enable local call features.

network-id

Configures the Network Identifier.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

network-id *id*

no network-id

id

The Network Identifier of the entity.
id must be from 1 to 79 alpha and/or numeric characters in length.

no

Removes the configured Network Identifier of the entity.

Usage

The Network Identifier is used to compare with the P-Visited-Network-ID header received from P-CSCF to decide home or roaming subscriber at S-CSCF service.

Example

Sets the Network Identifier to *pcscf01.company.com:*

```
network-id pcscf01.company.com
```

npdb-client

Creates an NPDB (Number Portability Data Base) client under CSCF and enters the CSCF NPDB Client Configuration Mode.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

npdb-client *client_name* **[-noconfirm]**

no npdb-client

client_name

Specifies the name of the NPDB client.
client_name must be from 1 to 79 alpha and/or numeric characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

no

Deletes NPDB client under CSCF.

Usage

Use this command to enable the NPDB client feature and enter the NPDB Client Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-npdb-client)#
```

NPDB Client Configuration Mode commands are defined in the *CSCF NPDB Client Configuration Mode Commands* chapter in this guide.

Example

The following command creates an NPDB client named *npdb1* and enters NPDB Client Configuration Mode:

```
npdb-client npdb1
```

policy

Configures the policy for Served User Routing in this S-CSCF service.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
[ default | no ] policy allow p-served-user-routing
```

default | no

Disables Served User Routing functionality for this S-CSCF.

allow p-served-user-routing

Enables Served User Routing functionality for this S-CSCF.

Usage

Use this command to enable/disable the policy for Served User Routing.

Example

The following command enables Served User Routing on this service:

```
policy allow p-served-user-routing
```

The following command disables Served User Routing on this service:

```
no policy allow p-served-user-routing
```

registration lifetime

Configures a registration lifetime for all subscribers to the service.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

registration lifetime { default *sec* **| implicit** *sec* **| max** *sec* **| min** *sec* **}**

default registration lifetime

{ default *sec* **| implicit** *sec* **| max** *sec* **| min** *sec* **}**

default *sec*: Specifies the default amount of time that a registration can exist on the system.
sec must be an integer from 60 to **max** *sec* -1.
Default: 3600

Important: **default** *sec* must be < or = to max *sec* and > or = to min *sec*.

implicit *sec*: Specifies the implicit amount of time that a registration can exist on the system. *sec* must be an integer from 60 to 1209600.
Default: 0
max *sec*: Specifies the maximum amount of time that a registration can exist on the system.
sec must be an integer from 60 to 1209600.
Default: 86400

Important: **max** *sec* must be > or = to min *sec*.

min *sec*: Specifies the minimum amount of time that a registration can exist on the system.
sec must be an integer from 60 to **max** *sec* -1.
Default: 60

Important: **min** *sec* must be < or = to max *sec*.

default

Returns the command to the default settings.

Usage

Use this command to control the amount of time registrations are allowed to exist on this service.
The system responds to registrations in the following manner:
If implicit-timer is configured (>0), and if UE expires time < min expires time, respond with 200 OK with Expires-header set to configured implicit-expires time.
If implicit timer is not configured (=0), the service will respond with a 423 Interval Too Small message.

Using default values:

- If a registration with an expiration value lower than the service's minimum (60) is received, the service will respond with a 423 Interval Too Small message.
- If a registration with an expiration value higher than the service's maximum (2147483646) is received, the service will automatically reduce the expiration value to the default value.
- If a registration is received missing the "Expires" value, or the value is malformed, the service will automatically respond with 3761 in the 200 OK message.

Example

The following command configures the maximum registration lifetime to *43200* (12 hours):

```
registration lifetime max 43200
```

reliable-prov-resp

Enables/disables the reliability of provisional responses feature.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

```
reliable-prov-resp { mandatory | optional }

no reliable-prov-resp
```

mandatory | optional

mandatory: Both inbound and outbound will request reliability.
optional (default): Reliability is imposed by inbound side. Only if inbound call requests reliability will outbound also request reliability.

no

Disables the reliability of provisional responses feature.

Usage

Use this command to enable/disable the reliability of provisional responses feature.

Example

The following command sets the reliability of provisional responses feature to mandatory:

```
reliable-prov-resp mandatory
```

server-name

Enables/disables filling the server name AVP in MAR and SAR for Cx interface with configured server name. This command is disabled by default.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

server-name *server_name*

no server-name

server_name

Configures the name that will be used to fill the server name AVP in MAR and SAR for Cx interface. *name* must be from 1 to 63 alpha and/or numeric characters.

no

S-CSCF uses configured cscf-hostname or bind IP address to fill the server name AVP in MAR and SAR for Cx interface. This is the default CSCF behavior.

Usage

Use this command to enable/disable filling the server name AVP in MAR and SAR for Cx interface with configured server name.

Example

The following command configures the CSCF server name as *stp-c-scscf1.cisco.co.kr*:

```
server-name stp-c-scscf1.cisco.co.kr
```

sifc

Enables Shared Initial Filter Criteria (SiFC) functionality. This command is disabled by default.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

```
[ default | no ] sifc
```

default | no

Disables shared iFC functionality for this S-CSCF.

Usage

Use this command to configure the S-CSCF to share iFC functionality.

Important: 48 SiFC IDs are supported per subscriber.

If both the HSS and the S-CSCF support this feature, subsets of iFC may be shared by several service profiles. The HSS downloads the unique identifiers of the shared iFC sets to the S-CSCF. The S-CSCF uses a locally administered database to map the downloaded identifiers onto the shared iFC sets.
If the S-CSCF does not support this feature, the HSS will not download identifiers of shared iFC sets.

Important: When using this feature option, the network operator is responsible for keeping the local databases in the S-CSCFs and HSSs consistent.

sip-header insert

Enable SIP header insertion for the S-CSCF service. SIP header insertion is disabled by default.

Product

SCM (S-CSCF)

Privilege

Administrator

Syntax

```
[ no ] sip-header insert { p-cust1-prid-info | p-user-database }
```

no

Disables specific SIP header insertion for the S-CSCF service.

p-cust1-prid-info

Inserts a custom header, P-LGUPlus-PRID-Info, which contains the private user id of the user sending the REGISTER request, to be added in the REGISTER message toward AS during third party registration.

p-user-database

Inserts PUD header in SIP (REGISTER) message and Invite from I-CSCF to S-CSCF.

Usage

Enabling this command allows header insertion in SIP (REGISTER) message.

Example

The following command disables insertion of custom header, P-LGUPlus-PRID-Info, in SIP (REGISTER) message:

```
no sip-header insert p-cust1-prid-info 5
```

The following command enables insertion of PUD header in SIP (REGISTER) message and Invite from I-CSCF to S-CSCF:

```
sip-header insert p-user-database 5
```

sip-request

Configures SIP Request-related configuration in this S-CSCF service.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

```
sip-request re-route { max-attempts attempts | response-code code }

default sip-request re-route max-attempts

no sip-request re-route response-code code
```

re-route

Specify SIP Request re-route related configuration.

max-attempts *attempts*

Specifies the maximum number of re-route attempts that a S-CSCF should allow for a given call before passing the negative response upstream.
attempts must be an integer from 1 to 10.
Default: 2

response-code *code*

Specifies the list of Response codes that will be considered as re-routable responses to a call attempt.
code must be a three-digit integer from 400 to 699.

Important: You may configure a maximum of five response code values per S-CSCF service.

default

Specifies a maximum number of two re-route attempts that a S-CSCF should allow for a given call before passing the negative response upstream.

no

Disables the specified Response code.

Usage

Use this command to configure:

- list of Response codes that will be considered as re-routable responses to a call attempt.
- the maximum number of re-route attempts that a S-CSCF should allow for a given call before passing the negative response upstream.

Example

The following command configures the maximum number of re-route attempts to *5*:

```
sip-request re-route max-attempts 5
```

tas

Configures the S-CSCF to perform Telephony Application Server (TAS) functions.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

```
[ default | no ] tas
```

default | no

Disables the TAS feature for this S-CSCF.

Usage

Use this command to configure the S-CSCF to perform TAS functions.

tas-service

Identifies the name of the service configured on the system performing Telephony Application Server (TAS) functions.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

tas-service *name*

no tas-service

name

Specifies the name of the service configured on the system performing TAS functions.
name must be from 1 to 63 alpha and/or numeric characters and be an existing service.

no

Removes the TAS name from the S-CSCF configuration.

Usage

Use this command to identify the name of the service configured on the system performing TAS functions

Example

The following command identifies the TAS service name as *scscf3*:

```
tas-service scscf3
```

user-authorization

Enables sending user-authorization to HSS. User-authorization is disabled by default.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

```
[ default | no ] user-authorization
```

default | no

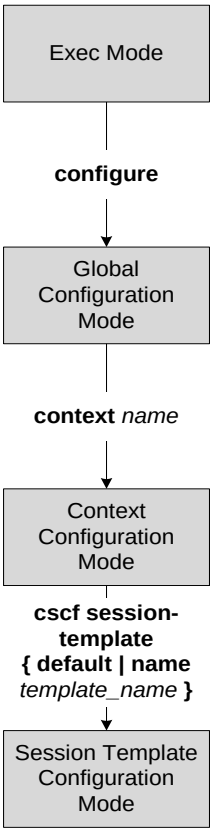
Disables sending user-authorization to HSS.

Usage

If this command is enabled, and I-CSCF role is enabled in S-CSCF, I-CSCF will send UAR/UAA diameter message to HSS.

Chapter 90
CSCF Session Template Configuration Mode Commands

The CSCF Session Template Configuration Mode is used to classify users and/or domains (AoRs) within the system.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

inbound-cscf-acl

Configures the ACL to use for inbound sessions using this template.

Product

SCM

Privilege

Administrator

Syntax

inbound-cscf-acl { default | name *acl_name* **}**

no inbound-cscf-acl name *acl_name*

default | name *acl_name*

default: Specifies that the default ACL should be used for inbound sessions using this template.
name *acl_name*: Specifies an existing ACL to use for inbound sessions using this template. *acl_name* must be the name of an existing ACL.

no inbound-cscf-acl name *acl_name*

Removes the ACL from this template.

Usage

Use this command to identify an ACL to use on inbound sessions using this template.

Example

The following command sets the inbound ACL for this template to an ACL named *acl_in22*:

```
inbound-cscf-acl name acl_in22
```

outbound-cscf-acl

Configures the ACL to use for outbound sessions using this template.

Product

SCM

Privilege

Administrator

Syntax

outbound-cscf-acl { default | name *acl_name* **}**

no outbound-cscf-acl name *acl_name*

default | name *acl_name*

default: Specifies that the default ACL should be used for outbound sessions using this template.
name *acl_name*: Specifies an existing ACL to use for outbound sessions using this template. *acl_name* must be the name of an existing ACL.

no outbound-cscf-acl name *acl_name*

Removes the ACL from this template.

Usage

Use this command to identify an ACL to use on outbound sessions using this template.

Example

The following command sets the outbound ACL for this template to an ACL named *acl_out22*:

```
outbound-cscf-acl name acl_out22
```

policy-profile

Configures an AoR policy group to be used for sessions using this template.

Product

SCM

Privilege

Administrator

Syntax

policy-profile { default | name *profile_name* **}**

no policy-profile name *profile_name*

default | name *profile_name*

default: Specifies that the default policy group will be used for sessions using this template.
name *profile_name*: Specifies an existing policy group. *profile_name* must be an existing CSCF policy group.

no policy-profile name *profile_name*

Removes the policy group from the template.

Usage

Use this command to specify a policy group for the template.

Example

The following command specifies that a policy group called *aor_grp1* will be used for sessions using this template:

```
policy-profile name aor_grp1
```

route-list

Configures a route group to be used for sessions using this template.

Product

SCM

Privilege

Administrator

Syntax

route-list { default | name *group_name* **}**

no route-list name *group_name*

default | name *group_name*

default: Specifies that the default route group will be used for sessions using this template.
name *group_name*: Specifies an existing route group. *group_name* must be an existing peer server group.

no route-list name *group_name*

Removes the route group from this template.

Usage

Use this command to specify a route group for the template.

Example

The following command specifies an accounting server group called *route_grp2* that will be used for sessions using this template:

```
route-list name route_grp2
```

translation-list

Configures a translation list to be used for sessions using this template.

Product

SCM

Privilege

Administrator

Syntax

translation-list { default | name *list_name* **}**

no translation-list name *list_name*

default | name *list_name*

default: Specifies that the default translation list will be used for sessions using this template.
name *list_name*: Specifies an existing translation list. *list_name* must be an existing translation list.

no translation-list name *list_name*

Removes the translation list from this template.

Usage

Use this command to specify a translation list for the template.

Example

The following command specifies a translation list called *trans_list6*:

```
translation-list name trans_list6
```

urn-service-list

Configures an URN service list to be used for sessions using this template.

Product

SCM

Privilege

Administrator

Syntax

urn-service-list { default | name *list_name* **}**

no urn-service-list name *list_name*

default | name *list_name*

default: Specifies that the default URN service list will be used for sessions using this template.
name *list_name*: Specifies an existing URN service list name. *list_name* must be from 1 to 79 alpha and/or numeric characters and be an existing URN service list.

no urn-service-list name *list_name*

Removes the service list from this template.

Usage

Use this command to specify a URN service list for this template. URN service lists are configured in the URN Service List Configuration Mode.

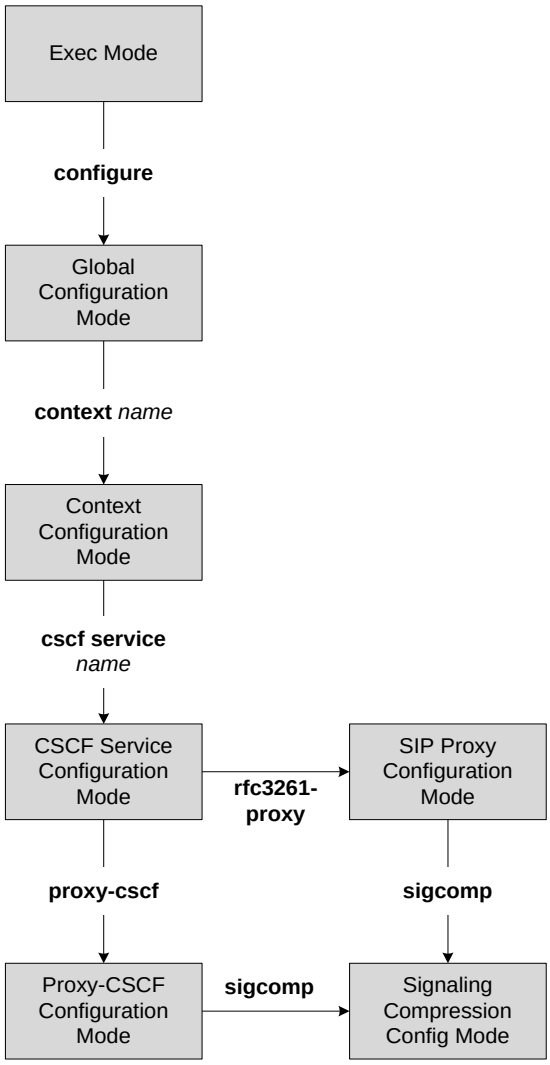
Example

The following command specifies that a URN service list named *urn_list5* will be used for sessions using this template:

```
urn-service-list name urn_list5
```

Chapter 91
CSCF Signalling Compression Configuration Mode Commands

The CSCF Signalling Compression Configuration Mode is used to set memory allocation parameters in support of SIP signalling compression. More information regarding signalling compression refer to the IETF RFC 3320 “Signaling Compression (SigComp)”.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

compression-mode

Configures the dynamic compression mode to be used while sending a SigComp message. Simple dynamic mode is the default.

Product

SCM

Privilege

Administrator

Syntax

```
compression-mode { multiple-dynamic | simple-dynamic | static | update-dynamic }

default compression-mode
```

multiple-dynamic | simple-dynamic | static | update-dynamic

Default: **simple-dynamic**
multiple-dynamic: A maximum of four dynamic states will be created per compartment. The dynamic states are updated for each message by deleting the oldest dynamic state and creating the new one. The dynamic states will be updated in FIFO (First In, First Out) order.
simple-dynamic: Only one dynamic state will be created per compartment. The same state will be used for compression.
static: No dynamic states will be created. Only static dictionary will be used for compression.
update-dynamic: Only one dynamic state will be created per compartment, but the dynamic state will be updated for every new message.

default compression-mode

Returns the dynamic compression mode to simple dynamic.

Usage

Use this command to configure the dynamic compression mode to be used.

Example

The following command sets the compression mode to multiple dynamic:

```
compression-mode multiple-dynamic
```

The following command completely disables the creation of dynamic states for compression:

```
compression-mode static
```

decompression-memory-size

Sets the amount of memory available for decompressing one SigComp message. A portion of the allocated memory is used to buffer the message before it is decompressed. The memory is allocated for each SigComp message and is reclaimed once decompression is completed.

Product

SCM

Privilege

Administrator

Syntax

```
decompression-memory-size { 128k | 16k | 32k | 64k | 8k }

default decompression-memory-size
```

128k | 16k | 32k | 64k | 8k

Default: **8k**
Specifies the amount of memory (in kilobytes) to allocate for decompressing one SigComp message.

default

Returns the command to the default settings.

Usage

Use this command to set the memory size used to decompress a single SigComp message.

Example

The following command sets the memory size for decompressing SigComp messages to 16k:

```
decompression-memory-size 16k
```

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

exit

Usage

Return to the previous mode.

state-memory-size

Sets the memory allocated to a compartment for the creation of state. Compartments are application-specific groupings of messages that relate to a peer endpoint. The system allocates memory per compartment. The memory is reclaimed when the system determines that the compartment is no longer required.

Product

SCM

Privilege

Administrator

Syntax

```
state-memory-size { 4k | 8k }

default state-memory-size
```

4k | 8k

Default: **4k**
Specifies the amount of memory to allocate to a compartment for the creation of state.

default

Returns the command to the default settings.

Usage

Use this command to specify a memory size allocated to message groupings for the creation of state.

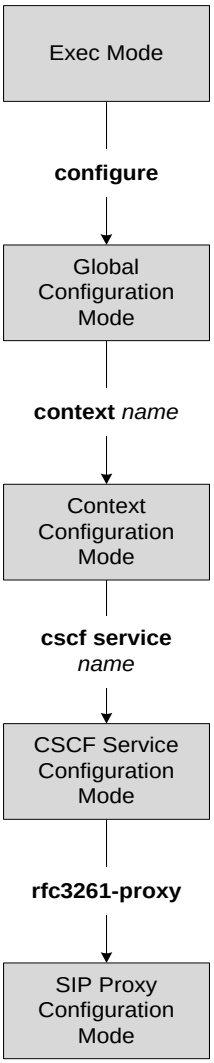
Example

The following command sets the state memory size to **8k**:

```
state-memory-size 8k
```

Chapter 92
CSCF SIP Proxy Configuration Mode Commands

The SIP Proxy Configuration Mode is used to set various commands supporting the role of the CSCF service as a RFC3261-compliant SIP proxy server.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

as-call

Enabling this command causes request-URIs in INVITE messages to be updated with the result of the translation before being passed to an Application Server. This command is disabled by default.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

```
[ default | no ] as-call invite-request-uri update
```

default | no

The translation result is ignored.

Usage

Use this command to update the request-URI in INVITE messages with the result of the translation before passing it to an AS.

authentication

Configures the authentication method used by the CSCF service.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

authentication { aka-v1 *value* **| allow-noauth [invite | re-register| register] | allow-noipauth [invite | re-register| register] | allow-unsecure | aor-auth | md5** *value* **}**

no authentication { aka-v1 | allow-noauth [invite | re-register| register] | allow-noipauth [invite | re-register| register] | allow-unsecure | aor-auth | md5 }

aka-v1 *value*

Specifies that AKA-v1 algorithm is used as the authentication type when accessing the CSCF service. *value* specifies a preference - the lower the value, the higher the preference. *value* must be an integer from 1 to 1000.

Important: In order to change a priority level, you must remove the original value and configure a new one.

allow-noauth [invite | re-register| register]

Specifies that access to the CSCF service is allowed if authentication fails.
invite: Specifies that access to the CSCF service is allowed if authentication fails on INVITE requests only.
re-register: Specifies that access to the CSCF service is allowed if authentication fails on RE-REGISTER requests when the request is integrity-protected only.
registration: Specifies that access to the CSCF service is allowed if authentication fails on REGISTER requests only.

allow-noipauth [invite | re-register| register]

Specifies that access to the CSCF service is allowed if early IMS-based IP authentication fails.
invite: Specifies that access to the CSCF service is allowed if early IMS-based IP authentication fails on INVITE requests only.
re-register: Specifies that access to the CSCF service is allowed if authentication fails on RE-REGISTER requests when the request is integrity-protected only.
registration: Specifies that access to the CSCF service is allowed if early IMS-based IP authentication fails on REGISTER requests only.

allow-unsecure

Specifies that un-secure access is allowed to the CSCF service.

aor-auth

Specifies that authentication is based on the AoR when accessing the CSCF service.

md5 *value*

Specifies that the MD5 algorithm is used as the authentication type for accessing the CSCF service. *value* specifies a preference - the lower the value, the higher the preference. *value* must be an integer from 1 to 1000.

Important: In order to change a priority level, you must remove the original value and configure a new one.

no authentication { aka-v1 | allow-noauth [invite | re-register| register] | allow-noipauth [invite | re-register| register] | allow-unsecure | aor-auth | md5 }

Disables the specified authentication method for the CSCF service.

Usage

Use this command to configure the authentication method used by the CSCF service.

Important: The S-CSCF supports multiple authorization schemes, but this requires disabling all authorization configured in the S-CSCF service so that it will send "Unknown" in the Sip-Authorization-Scheme AVP. This allows the HSS to dictate authorization. The following commands disable all authorization configured in the S-CSCF service to allow HSS to control authorization:

```
authentication allow-noipauth

allow rfc3261-ua-interworking

no authentication aka-v1

no authentication md5
```

Example

The following command configures the authentication method used by the CSCF service to MD5 with a preference of *3*:

```
authentication md5 3
```

diversion-info

Enabling this command prompts the service to add a diversion header (draft-levy-sip-diversion-08) when the call is diverted to a different endpoint due to a call feature. By default diversion-info is disabled.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

```
[ default | no ] diversion-info
```

default | no

The service will not add a diversion header.

Usage

Use this command to enable the service to add a diversion header to call setup packets when calls are diverted due to the application of call features.

emergency

Configures the function to allow or disallow the emergency-session or emergency-registration of a particular type.

Product

SCM (P-CSCF, A-BG, SIP Proxy)

Privilege

Administrator

Syntax

```
[ default | no ] emergency { registration [ visited-ue ] | session [ 3gpp-ims-xml-body |
anonymous | non-emergency-registered | sdp-cs-media | visited-ue ] }
```

default

Specifies that the emergency-session or emergency-registration of a particular type can be allowed.

no

Disallows the emergency-session or emergency-registration of a particular type.

registration

Allow emergency-registration. By default, it's allowed.
visited-ue: Allow emergency-registration from a visited UE. By default, it's allowed.

session

Specifies the type of emergency-session to be allowed or disallowed. By default, all are allowed.
3gpp-ims-xml-body: Allow 3GPP IM CN XML body to be added in 380 response messages.
anonymous: Allow anonymous subscribers (unregistered UEs) to initiate emergency sessions.
non-emergency-registered: Allow non-emergency registered subscribers to initiate emergency sessions.
sdp-cs-media: Allow emergency calls with SDP CS Media.
visited-ue: Allow emergency calls from visited UE.

Usage

Use this command to configure the function to allow or disallow the emergency-session or emergency-registration of a particular type.

Example

The following command configures the function to allow non-emergency registered subscribers to initiate emergency sessions:

```
emergency session non-emergency-registered
```

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

```
exit
```

Usage

Return to the previous mode.

registration

Configures a registration lifetime for all subscribers to the service.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

registration lifetime { default *sec* **| max** *sec* **| min** *sec* **}**

default registration lifetime

{ default *sec* **| max** *sec* **| min** *sec* **}**

default *sec*: Specifies the default amount of time that a registration can exist on the system. *sec* must be an integer from 60 to **max** *sec* -1. Default is 3600. default *sec* must be < or = to max *sec* and > or = to min *sec*.
max *sec*: Specifies the maximum amount of time that a registration can exist on the system. *sec* must be an integer from 60 to 1209600. Default is 86400. max *sec* must be > or = to min *sec*.
min *sec*: Specifies the minimum amount of time that a registration can exist on the system. *sec* must be an integer from 60 to **max** *sec* -1. Default is 60. min *sec* must be < or = to max *sec*.

---

default registration lifetime

Returns the command to the default settings.

Usage

Use this command to control the amount of time registrations are allowed to exist on this service.
The system responds to registrations in the following manner:
Using default values:

- If a registration with an expiration value lower than the service's minimum (60) is received, the service will respond with a 423 Interval Too Small message.
- If a registration with an expiration value higher than the service's maximum (2147483646) is received, the service will automatically reduce the expiration value to the default value.
- If a registration is received missing the "Expires" value, or the value is malformed, the service will automatically respond with 3761 in the 200OK message.

Example

The following command configures the maximum registration lifetime to *43200* (12 hours):

```
registration lifetime max 43200
```

reliable-prov-resp

Enables/disables the reliability of provisional responses feature.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

```
reliable-prov-resp { mandatory | optional }

no reliable-prov-resp
```

mandatory | optional

mandatory: Both inbound and outbound will request reliability.
optional (default): Reliability is imposed by inbound side. Only if inbound call requests reliability will outbound also request reliability.

no

Disables the reliability of provisional responses feature.

Usage

Use this command to enable/disable the reliability of provisional responses feature.

Example

The following command sets the reliability of provisional responses feature to mandatory:

```
reliable-prov-resp mandatory
```

The following command disables the reliability of provisional responses feature:

```
no reliable-prov-resp
```

sifc

Enables Shared Initial Filter Criteria (SiFC) functionality. This command is disabled by default.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

```
[ default | no ] sifc
```

default | no

Disables shared iFC functionality for this SIP Proxy.

Usage

Use this command to configure the SIP Proxy to share iFC functionality.
If both the HSS and the SIP Proxy support this feature, subsets of iFC may be shared by several service profiles. The HSS downloads the unique identifiers of the shared iFC sets to the SIP Proxy. The SIP Proxy uses a locally administered database to map the downloaded identifiers onto the shared iFC sets.
If the SIP Proxy does not support this feature, the HSS will not download identifiers of shared iFC sets.

Important: When using this feature option, the network operator is responsible for keeping the local databases in the S-CSCFs and HSSs consistent.

sigcomp

Enables signaling compression for the SIP Proxy service and enters the Signaling Compression Configuration Mode.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

```
[ no ] sigcomp
```

no

Disables signaling compression for the CSCF service.

Usage

Use this command to enable signaling compression for the SIP Proxy service and enter the CSCF Signaling Compression Configuration Mode.
Entering this command results in the following prompt:

```
[context_name]hostname(config-sigcomp)#
```

Signaling Compression Configuration Mode commands are defined in the *CSCF Signaling Compression Configuration Mode Commands* chapter in this guide.

tas

Configures the SIP Proxy to perform Telephony Application Server (TAS) functions.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

```
[ default | no ] tas
```

default | no

Disables the TAS feature for this SIP Proxy.

Usage

Use this command to configure the SIP Proxy to perform TAS functions.

tas-service

Identifies the name of the service configured on the system performing Telephony Application Server (TAS) functions.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Administrator

Syntax

tas-service *name*

[default | no] tas-service

name

Specifies the name of the service configured on the system performing TAS functions. *name* must be from 1 to 63 alpha and/or numeric characters and be an existing service.

default | no

Removes the TAS name from the SIP Proxy configuration.

Usage

Use this command to identify the name of the service configured on the system performing TAS functions. The ims-sh-service commands are defined in the Context Configuration Mode Commands chapter in this guide.

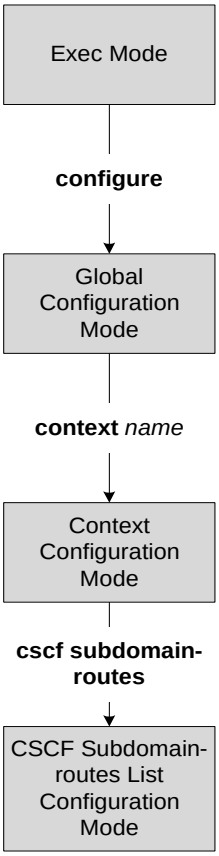
Example

The following command identifies the TAS service name as *scscf3*:

```
tas-service scscf3
```

Chapter 93
CSCF Subdomain-route List Configuration Mode Commands

The CSCF Subdomain-route List Configuration Mode is used to configure the subdomain-routes for the I-CSCF. These subdomain-routes are used to send messages over the Ma-interface (I-CSCF interface toward AS).



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

after

Places the subdomain-route at the bottom or end of the subdomain-routes list. Use this command in conjunction with the **route** command.

Product

SCM (I-CSCF)

Privilege

Administrator

Syntax

after

Usage

Add this command before the **route** command to place the route at the end of the subdomain-routes list.

before

Places the subdomain-route at the beginning or top of the subdomain-routes list. Use this command in conjunction with the **route** command.

Product

SCM (I-CSCF)

Privilege

Administrator

Syntax

before

Usage

Add this command before the **route** command to place the route at the beginning of the subdomain-routes list.

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

exit

Usage

Return to the previous mode.

route

Creates a route entry to be used in the subdomain-routes list for the I-CSCF.

Product

SCM (I-CSCF)

Privilege

Administrator

Syntax

`[ no ] route peer-servers` *`name`* **`[ log ] base-criteria destination aor`** *`aor`*

`no`

Removes specified route entry.

`peer-servers` *`name`*

Specifies the name of a peer server group.
`name` must be an existing peer server group from 1 to 79 alpha and/or numeric characters in length.

`log`

Enables logging for CSCF sessions meeting the criteria specified. The logs can be viewed by executing the **`logging filter active facility cscf`** command in the Exec mode.

`base-criteria destination aor` *`aor`*

Filters routes based on the destination AoR.
`aor` must be an existing AoR from 1 to 79 alpha and/or numeric characters in length.

Important: AoR regular expressions are supported. Refer to the *SCM Engineering Rules* Appendix in the *Session Control Manager Administration Guide* for more information about regular expressions.

Usage

Use this command to create and order routes in the subdomain-routes list for the I-CSCF. I-CSCF, upon receiving the terminating request, checks the subdomain-route list for matches. If a match is found, the routing will happen based on it. Otherwise, I-CSCF performs a User Location Query (Location-Information-Request) before proceeding.

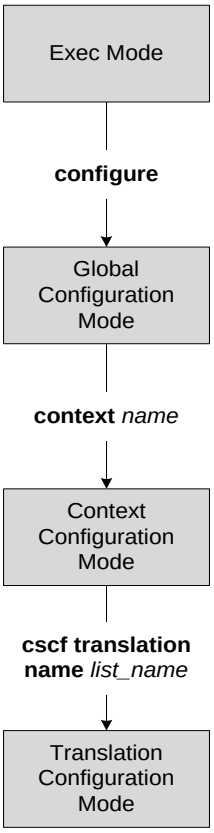
Example

The following command creates a route for the subdomain-routes list to peer server group *`ps5`* with a destination AoR of *`$.@abc123.com`*:

```
route peer-servers ps5 base-criteria destination aor $.@abc123.com
```

Chapter 94
CSCF Translation Configuration Mode Commands

The CSCF Translation Configuration Mode is used to configure session re-addressing within the system.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

after

Places the CSCF translation entry at the bottom or end of the translation list. Use this command in conjunction with the **uri-readdress** command.

Product

SCM

Privilege

Administrator

Syntax

after

Usage

Add this command before the **uri-readdress** command to place the entry at the end of the translation list.

before

Places the CSCF translation entry at the top or beginning of the translation list. Use this command in conjunction with the **uri-readdress** command.

Product

SCM

Privilege

Administrator

Syntax

before

Usage

Add this command before the **uri-readdress** command to place the entry at the beginning of the translation list.

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax

exit

Usage

Return to the previous mode.

uri-readdress

Configures readdress criteria for URI translations.

Product

SCM

Privilege

Administrator

Syntax

uri-readdress type *trans_type* **[log] { base-criteria** *criteria* **} [filter-criteria1** *criteria* **] [filter-criteria2** *criteria* **]**

no uri-readdress type *trans_type* **{ base-criteria** *criteria* **} [filter-criteria1** *criteria* **] [filter-criteria2** *criteria* **]**

---

type *trans_type*

Specifies that the translation list (*trans_type*) entry is to be identified as one of the following:
blocking-cid: Identifies the translation list entry type as “call ID blocking”.
cancel-blocking-cid: Identifies the translation list entry type as “cancel call ID blocking”.
cancel-cid: Identifies the translation list entry type as “cancel call ID display”.
cancel-cw: Identifies the translation list entry type as “cancel call-waiting”.
cfbl-off: Identifies the translation list entry type as “call forward busy line off”.
cfbl-on: Identifies the translation list entry type as “call forward busy line on”.
cfna-off: Identifies the translation list entry type as “call forward no answer off”.
cfna-on: Identifies the translation list entry type as “call forward no answer on”.
cfu-off: Identifies the translation list entry type as “call forward unconditional off”.
cfu-on: Identifies the translation list entry type as “call forward unconditional on”.
cid: Identifies the translation list entry type as “call ID display”.
cw-off: Identifies the translation list entry type as “call-waiting off”.
cw-on: Identifies the translation list entry type as “call-waiting on”.
directory-assistance: Identifies the translation list entry type as “directory assistance”.
emergency: Identifies the translation list entry type as “emergency”.
international: Identifies the translation list entry type as “international”.
local: Identifies the translation list entry type as “local”.
long-distance: Identifies the translation list entry type as “long-distance”.
none: Identifies the translation list entry type as “any”.
operator-assistance: Identifies the translation list entry type as “operator assistance”.
premium-service: Identifies the translation list entry type as “premium service”.
service: Identifies the translation list entry type as “special service”.
tollfree: Identifies the translation list entry type as “toll free”.

---

log

Enables logging for CSCF sessions meeting the readdress criteria for URI translations.

---

base-criteria *criteria*

Specifies the base criteria that packets will be compared against. The following criteria is supported:

- **any**: Filters all CSCF sessions.

- **destination aor** *aor*: Filters sessions based on the destination AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

- **plmn-id mcc** *mcc_code* **mnc** *mnc_code*: Filters sessions based on the mobile country and network codes. *mcc_code* must be a three-digit integer from 200 to 999. *mnc_code* must be either a two or three-digit integer from 00 to 999 or **any** (any MNC code).
- **source address** *ip_address*: Filters sessions based on source IP address. *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
- **source aor** *aor*: Filters sessions based on the source AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

filter-criteria1 *criteria*

Specifies the filter criteria that packets that have passed the base criteria will be compared against. The following criteria is supported:

- **any**: Filters all CSCF sessions.
- **destination aor** *aor*: Filters sessions based on the destination AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

- **plmn-id mcc** *mcc_code* **mnc** *mnc_code*: Filters sessions based on the mobile country and network codes. *mcc_code* must be a three-digit integer from 200 to 999. *mnc_code* must be either a two or three-digit integer from 00 to 999 or **any** (any MNC code).
- **source address** *ip_address*: Filters sessions based on source IP address. *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
- **source aor** *aor*: Filters sessions based on the source AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

filter-criteria2 *criteria*

Specifies the filter criteria that packets that have passed the base criteria and filter criteria1 will be compared against. The following criteria is supported:

- **any**: Filters all CSCF sessions.
- **destination aor** *aor*: Filters sessions based on the destination AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

- **plmn-id mcc** *mcc_code* **mnc** *mnc_code*: Filters sessions based on the mobile country and network codes. *mcc_code* must be a three-digit integer from 200 to 999. *mnc_code* must be either a two or three-digit integer from 00 to 999 or **any** (any MNC code).

- **source address** *ip_address*: Filters sessions based on source IP address. *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
- **source aor** *aor*: Filters sessions based on the source AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

no uri-readdress type *trans_type* **{ base-criteria** *criteria* **} [filter-criteria1** *criteria* **] [filter-criteria2** *criteria* **]**

Remove the readdress configuration.

Usage

Use this command to readdress URIs based on specified criteria and enters the URI Readdress Configuration Mode. Readdressing can be used for:

- **Mobility**: When roaming in a visited domain.
- **Service Aliases**: Resolving well-known addresses via SIP-AS.
- **Number Translation**: Adding or deleting prefixes such as +1 to/from PSTN numbers.
- **Voice VPNs**: Using inter-office extensions to dial remote offices.

Entering this command results in the following prompt:

```
[context_name]hostname(config-uri-readdress)#
```

URI readdress commands are defined in the *CSCF URI Readdress Configuration Mode Commands* chapter of this reference.

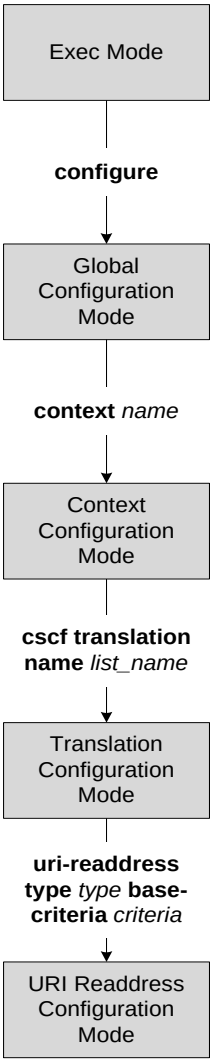
Example

The following command readdresses sessions to a domain named *service.com*, filters sessions with a base criteria of the source address (*1.2.3.4*) and a filter criteria of the destination AoR (*$.@test.com*):

```
uri-readdress type service base-criteria source address 1.2.3.4 filter-
criteria1 destination aor $.@test.com
```

Chapter 95
CSCF URI Readdress Configuration Mode Commands

The URI Readdress Configuration Mode is used to set URI translations.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

action

Adjusts a target address to route sessions to appropriate locations.

Product

SCM

Privilege

Administrator, Config-administrator

Syntax

```
action { add string | delete num_chars | modify string } position num length length
target { destination | source } { aor | domain | user }

no action
```

add *string* **| delete** *num_chars* **| modify** *string*

add *string*: Adds a specified string to a location indicated by the **position** keyword for the targeted source or destination address component (aor, domain, or user). *string* must be from 1 to 79 alpha and/or numeric characters.
delete *num_chars*: Deletes a number of characters starting from a location specified by the **position** keyword for the targeted source or destination address component (aor, domain, or user). *num_chars* must be an integer from 1 to 79.
modify *string*: Modifies a specified string in a location starting with the **position** keyword for the targeted source or destination address component (aor, domain, or user). The number of characters in the *string* variable will replace the same number in the address. *string* must be from 1 to 79 alpha and/or numeric characters.

position *num*

Specifies the position in the target string where the action is to occur. *num* must be an integer from 1 to 79.

length *length*

Specifies the length of the target string where the action is to occur. *length* must be an integer from 1 to 79.

Important: The **length** keyword is only supported in **modify** actions.

target { destination | source }

Species that the action is to occur within the source or destination address.

aor | domain | user

aor: Specifies that the action is applied to AoRs in the targeted source or destination address.
domain: Specifies that the action is applied to domains in the targeted source or destination address.
user: Specifies that the action is applied to users in the targeted source or destination address.

no

Disables target address to route sessions.

Usage

Use this command to manipulate SIP packets matching the criteria in the uri-readdress command.

Example

The following command prepends a “+1” to a destination AoR:

```
action add +1 position 1 target destination aor
```

The following command removes the first two characters from the destination AoR:

```
action delete 2 position 1 target destination aor
```

The following command replaces characters 2 through 4 with the characters “abc” in the destination AoR:

```
action modify abc position 2 target destination aor
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

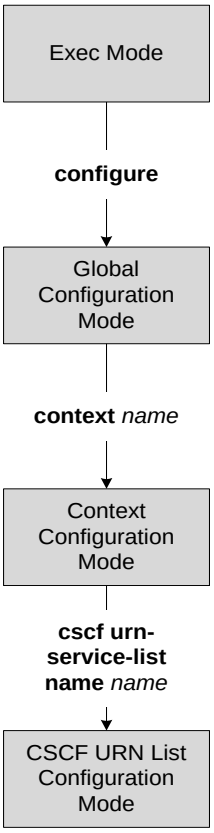
```
exit
```

Usage

Use this command to return to the parent configuration mode.

Chapter 96
CSCF URN List Configuration Mode Commands

The CSCF URN List Configuration Mode is used to map URNs to URIs for emergency and local call services.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

cscf-urn-service-mapping

Adds an entry to the service URN mapping table that maps uniform resource names (URNs) to URIs in order to direct specific service-oriented identifiers to the proper location in a network. The table is used after CSCF translation if the result is a local service.

Product

SCM

Privilege

Administrator

Syntax

`[ no ] cscf-urn-service-mapping urn` *`urn`* **`uri`** *`uri`*

`no`

Removes an entry from the service URN mapping table.

`urn` *`urn`*

Specifies the URN to be routed via a URL to the appropriate destination. *`urn`* must be from 1 to 79 alpha and/or numeric characters.

`uri` *`uri`*

Specifies the URI used to route the URN to the appropriate location. *`uri`* must be from 1 to 79 alpha and/or numeric characters.

Usage

Use this command to add an entry to the service URN mapping table that routes a translated URN to a URI for local services.

Important: Service URN mapping tables are limited to 30 URN to URI mapping entries.

Example

The following command map URN *`business`* to URI *`corp@123.45.678.9:5020`* and adds it to the service URN mapping table:

```
cscf-urn-service-mapping urn business uri corp@123.45.678.9:5020
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

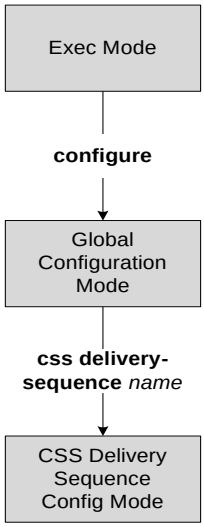
Usage

Use this command to return to the parent configuration mode.

Chapter 97
CSS Delivery Sequence Configuration Mode Commands

The CSS Delivery Sequence Configuration Mode is used to configure the order in which traffic is delivered to Content Service Steering (CSS) services and their associated content servers.

Important: This is a restricted configuration mode. In 9.0 and later releases, this configuration mode is deprecated.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

This is a restricted command. In 9.0 and later releases, this command is deprecated.

exit

This is a restricted command. In 9.0 and later releases, this command is deprecated.

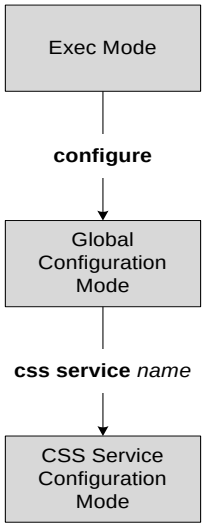
redirect service (any)

This is a restricted command. In 9.0 and later releases, this command is deprecated.

Chapter 98
CSS Service Configuration Mode Commands

The CSS Service Configuration Mode is used to configure properties for Content Service Steering (CSS) services. A CSS service binds a set of delivery interfaces to a service name and specifies a recovery mechanism.

Important: This is a restricted configuration mode. In 9.0 and later releases, this configuration mode is deprecated.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

This is a restricted command. In 9.0 and later releases, this command is deprecated.

exit

This is a restricted command. In 9.0 and later releases, this command is deprecated.

recovery

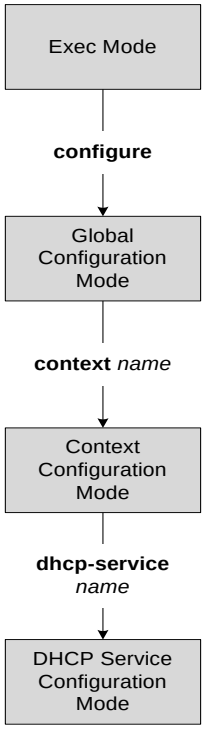
This is a restricted command. In 9.0 and later releases, this command is deprecated.

server-interface

This is a restricted command. In 9.0 and later releases, this command is deprecated.

Chapter 99
DHCP Service Configuration Mode Commands

The Dynamic Host Control Protocol (DHCP) Configuration Mode is used to create and manage DHCP service instances for the current context.



allow

Allows the specified options on the DHCP service.

Product

P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] allow { dhcp-inform | dhcp-relay-agent-auth-suboption | dhcp-relay-agent-option |
dhcp-server rapid-commit }
```

no

Disables an option on the DHCP service.

dhcp-inform

Enables the sending of DHCP inform after configuration for address recovery.

dhcp-relay-agent-auth-suboption

Enables the sending of DHCP relay agent authentication suboption in all outgoing messages.

dhcp-relay-agent-option

Enables the sending of DHCP relay agent option in all outgoing messages.

dhcp-server rapid-commit

Enables support of the rapid commit feature for DHCP server functionality, as defined in RFC 4039.

Usage

Use this command to enable/disable options on the DHCP service.

Example

The following command enables support of the rapid commit feature for DHCP server functionality:

```
allow dhcp-server rapid-commit
```

bind

Binds the DHCP service to a logical IP interface facilitating the system's connection to the DHCP server. This command also configures traffic from the specified DHCP service bind address to use the specified Multiple Protocol Label Switching (MPLS) labels.

Product

GGSN, ASN-GW, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
bind address ip_address [ nexthop-forwarding-address nexthop_ip_address [ mpls-label
input in_mpls_label_value output out_mpls_label_value1 [ out_mpls_label_value2 ] ] ]

no bind address ip_address
```

no

Removes a previously configured binding.

address *ip_address*

Specifies the IP address of an interface in the current context through which the communication with the DHCP server occurs. *ip_address* must be expressed in IPv4 dotted-decimal notation.

nexthop-forwarding-address *nexthop_ip_address*

Specifies the next hop gateway address for in MPLS network to which the packets with MPLS labels will be forwarded. *nexthop_ip_address* must be expressed in IPv4 dotted-decimal or IPv6 colon-separated notation.

mpls-label input *in_mpls_label_value*

Specifies the MPLS label to identify inbound traffic destined for the configured DHCP service bind address *ip_address*.
in_mpls_label_value is the MPLS label that will identify inbound traffic destined for the configured DHCP service and must be an integer from 16 through 1048575.

Important: This keyword is license-enabled and available with valid MPLS feature license only.

Caution: For DHCP over MPLS feature to work in StarOS 9.0 onward the **dhcp ip vrf** command must be configured in DHCP service. Without **dhcp ip vrf** command the DHCP service using MPLS labels will not be started as a part of a DHCP over MPLS configuration. In StarOS 9.0 onward this keyword is a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-service restart and clearing of the existing calls.

output *out_mpls_label_value1* **[** *out_mpls_label_value2* **]**

Adds the MPLS label to the outbound traffic sent from the configured DHCP service bind address *ip_address*. The labels *out_mpls_label_value1* and *out_mpls_label_value2* identify the MPLS labels to be added to packets sent from the specified dhcp service bind address.

out_mpls_label_value1 is the inner output label and must be an integer from 16 through 1048575.
out_mpls_label_value2 is the outer output label and must be an integer from 16 through 1048575.

Important: This keyword is license-enabled and available with valid MPLS feature license only.

Usage

Use this command to associate or tie the DHCP service to a specific logical IP address previously configured in the current context and bound to a port. Once bound, the logical IP address or interface is used in the giaddr field of the DHCP packets.
When this command is executed, the DHCP service is started and begins the process of requesting addresses from the DHCP server and storing them in cache memory for allocation to PDP contexts.
This command can also be used to configure MPLS labels for inbound and outbound traffic through this DHCP address.
Only one interface can be bound to a service.
For DHCP over MPLS feature to work in StarOS 9.0 onward **dhcp ip vrf** command must be configured in DHCP service. Without **dhcp ip vrf** command the DHCP service using MPLS labels will not be started.

Caution: As a part of DHCP over MPLS configuration, the **mpls-label input** keyword in the **bind address** command is also a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-service restart and clearing of the existing calls.

Example

The following command binds the DHCP service to the interface with an IP address of 1*92.168.1.210*:

```
bind address 192.168.1.210
```

default

Restores DHCP service parameters to their factory default settings.

Product

GGSN, ASN-GW, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

default { T1-threshold | T2-threshold | dhcp { chaddr-validate | client-identifier | deadtime | detect-dead-server { consecutive-failures } | server selection-algorithm } | lease-duration | max-retransmissions | retransmission-timeout }

---

dhcp { deadtime | detect-dead-server { consecutive-failures } | server-selection-algorithm }

Restores the following DHCP parameters to their respective default settings:

- **deadtime**: Default 10 minutes
- **detect-dead-server** { **consecutive-failures** }: Default 5
- **server-selection-algorithm**: Default First-server

---

lease-duration

Restores the lease-duration parameter to its default setting of 86400 seconds.

---

max-retransmissions

Restores the max-retransmissions parameter to its default setting of 5.

---

retransmission-timeout

Restores the retransmission-timeout parameter to its default setting of 3000 milli-seconds.

T1-threshold

Restores the T1-threshold parameter to its default setting of 50%.

T2-threshold

Restores the T2-threshold parameter to its default setting of 88%.

Usage

After system parameters have been modified, this command is used to set/restore specific parameters to their default values.

Example

The following command restores the DHCP deadtime parameter to its default setting of 10 minutes:

```
default dhcp deadtime
```

dhcp chaddr-validate

Configures the behavior of the client hardware address (chaddr) validation in DHCP messages.

Product

GGSN, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] dhcp chaddr-validate
```

default

Validates the chaddr value received in a DHCPACK message with the chaddr value sent in a DHCPREQUEST message.

no

Disables validation of the chaddr value received in DHCPACK message with the chaddr value sent in a DHCPREQUEST message.

Important: The chaddr information value in the DHCPACK message will be parsed but not be validated against the value maintained with client. The chaddr information value in DHCPACK will be ignored and not be stored internally.

Usage

Use this command to configure behavior relating to the validation of chaddr information validation in the DHCPACK messages.

Example

The following command specifies that the chaddr will not be validated in the DHCP messages:

```
no dhcp chaddr-validate
```

dhcp client-identifier

Configures the behavior relating to inclusion of a client identifier DHCP option in DHCP messages.

Product

GGSN, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
dhcp client-identifier { mac-address | msisdn | none }

default dhcp client-identifier
```

default

Sets the behavior of DHCP client identifier to default – do not to include client identifier option in any DHCP message.

mac-address

Specifies the subscribers mac-address as the DHCP client-identifier option in any DHCP message.

msisdn

Specifies that the subscriber's MSISDN be included in the client-identifier option of the relevant DHCP messages. Default: disabled

Important: This keyword is GGSN license controlled.

none

Specifies that DHCP client-identifier option would not be included in any DHCP messages. This is the default behavior. Default: enabled

Usage

Use this command to configure behavior relating to inclusion or exclusion of DHCP client identifier option from DHCP messages.

Example

The following command specifies that DHCP client-identifier option be excluded from DHCP messages:

```
dhcp client-identifier none
```

dhcp deadtime

Configures the amount of time that the system waits prior to re-communicating with a DHCP server that was previously marked as down.

Product

GGSN, ASN-GW, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

dhcp deadtime *max_time*

max_time

Specifies the maximum amount of time (in minutes) to wait before communicating with a DHCP server that was previously unreachable. *max_time* is an integer value from 1 through 65535. Default: 10

Usage

If the system is unable to communicate with a configured DHCP server, after a pre-configured number of failures the system marks the server as being down.
This command specifies the amount of time that the system waits prior to attempting to communicate with the downed server.

Important: If all DHCP servers are down, the system will immediately treat all DHCP servers as active, regardless of the deadtime that is specified.

Refer to the **dhcp detect-dead-server** and **max-retransmissions** commands for additional information on the process the system uses to mark a server as down.

Example

The following command configures the system to wait *20* minutes before attempting to re-communicate with a dhcp server that was marked as down:

```
dhcp deadtime 20
```

dhcp detect-dead-server

Configures the number of consecutive communication failures that could occur before the system marks a DHCP server as down.

Product

GGSN, ASN-GW, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

dhcp detect-dead-server consecutive-failures *max_number*

consecutive-failures *max_number*

Specifies the number of failures that could occur before marking a DHCP server as down as an integer from 1 through 1000. Default: 5

Usage

This command works in conjunction with the *max-retransmissions* parameter to set a limit to the number of communication failures that can occur with a configured DHCP server.
The *max-retransmissions* parameter limits the number of attempts to communicate with a server. Once that limit is reached, the system treats it as a single failure. This parameter limits the number of consecutive failures that can occur before the system marks the server as down and communicate with the server of next highest priority.
If all of the configured servers are down, the system ignores the detect-dead-server configuration and attempt to communicate with highest priority server again.
If the system receives a message from a DHCP server that was previously marked as down, the system immediately treats it as being active.

Example

The following command configures the system to allow *8* consecutive communication failures with a DHCP server before it marks it as down:

```
dhcp detect-dead-server consecutive-failures 8
```

dhcp ip vrf

Enables DHCP-over-MPLS support and associates the specific DHCP service with a pre-configured Virtual Routing and Forwarding (VRF) Context instance for virtual routing and forwarding.

Product

All

Privilege

Security Administrator, Administrator

Syntax

dhcp ip vrf *vrf_name*

no dhc ip vrf

no

Removes/disassociates configured IP Virtual Routing and Forwarding (VRF) context instance.

vrf_name

Specifies the name of a pre-configured VRF context instance to be associated with a DHCP service. *vrf_name* is the name of a pre-configured VRF context configured in Context Configuration mode and associated with the IP Pool used by the DHCP service.

Usage

Use this command to enable the DHCP-over-MPLS support and to associate/disassociate a pre-configured VRF context to a DHCP service for this feature.
By default the VRF is NULL, which means that DHCP service is bound with binding address given by **bind address** command only.
VRF is not a critical parameter for the DHCP Service but bind address is a critical parameter for DHCP Service, and while starting DHCP Service, if this command is configured, then the bind address should be present in that VRF, and If this command is not configured, bind address should be present in the context where DHCP Service is configured.
For the DHCP over MPLS feature to work in StarOS 9.0 onward this command must be configured in the DHCP service. Without this command the DHCP service using MPLS labels will not be started.

Caution: As a part of this configuration the **mpls-label input** keyword in the **bind address** command is also a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-service restart and clearing of the existing calls.

Example

Following command associates VRF context instance *dhcp_vrf1* with this DHCP service:

```
dhcp ip vrf dhcp_vrf1
```

dhcp server

Configures DHCP servers with which the DHCP service is to communicate.

Product

GGSN, ASN-GW, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

dhcp server *ip_address* **[priority** *priority* **]**

no dhcp server *ip_address*

no

Deletes a previously configured DHCP server.

ip_address

Specifies the IP address of the DHCP server expressed in IPv4 dotted-decimal notation.

priority *priority*

Specifies the priority of the server if multiple servers are configured. *priority* is an integer from 1 through 1000. 1 is the highest priority.

Usage

Use this command to configure the DHCP server(s) that the system is to communicate with. Multiple servers can be configured each with their own priority. Up to 20 DHCP servers can be configured.
All DHCP messages are sent/received on UDP port 67.

Important: If a server is removed, all calls having an IP address allocated from the server will be released.

Example

The following command configures a DHCP server with an IP address of *192.168.1.200* and a priority of *1*:

```
dhcp server 192.168.1.200 priority 1
```

dhcp server selection-algorithm

Specifies the algorithm used to select DHCP servers with which to communicate when multiple servers are configured.

Product

GGSN, ASN-GW, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
dhcp server selection-algorithm { first-server | round-robin }
```

first-server

Uses the first-server algorithm. This algorithm dictates that the system select the DHCP servers according to their priority starting with the highest priority server. The system communicates with the server of the next highest priority only when the previous server is unreachable. Default: Enabled

round-robin

Uses the round-robin algorithm. This algorithm dictates that the system communicates with the servers in a circular queue according to the server's configured priority starting with the highest priority server. The next request is communicated with the next highest priority server, and so on until all of the servers have been used. At this point, the system starts from the highest priority server. Default: Disabled

Usage

Use this command to determine how configured DHCP servers are utilized by the system.

Example

The following command configures the DHCP service to use the round-robin selection algorithm:

```
dhcp server selection-algorithm round-robin
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

lease-duration

Configures the minimum and maximum allowable lease times that are accepted in responses from DHCP servers.

Product

GGSN, ASN-GW, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

lease-duration min *min_time* **max** *max_time*

min *min_time*

Specifies the minimum acceptable lease time (in seconds) as an integer from 600 trough 3600. Default: 600

max *max_time*

Specifies the maximum acceptable lease time (in seconds) as an integer from 10800 through 4294967295. Default: 86400

Usage

To reduce the call setup time, the system requests IP addresses from the DHCP server in blocks rather than on a call-by-call basis. Each address received has a corresponding lease time, or time that it is valid. The values configured by command represent the minimum and maximum times that the system allows and negotiates for the lease(s).

If the DHCP server responds with values that are out of the range specified by the min and max values, the system accumulates warning statistics. Responses that fall below the minimum value are rejected by the system and the system contacts the DHCP server with the next highest priority. Responses that are greater than the maximum value are accepted.

When half of the lease time has expired, the system automatically requests a lease renewal from the DHCP server. This is configured using the **T1-threshold** command.

Example

The following command configures the minimum allowable lease time for the system to be *1000* and the maximum to be *36000*:

```
lease-duration min 1000 max 36000
```

max-retransmissions

Configures the maximum number of times that the system attempts to communicate with an unresponsive DHCP server before it is considered a failure.

Product

GGSN, ASN-GW, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

max-retransmissions *max_number*

max_number

Specifies the maximum number of re-attempts the system tries when no response is received from a DHCP server. *max_number* is an integer from 1 through 20. Default: 5

Usage

This command works in conjunction with the *dhcp detect-dead-server* parameter to set a limit to the number of communication failures that can occur with a configured DHCP server.
When the value specified by this parameter is met, a failure is logged. The *dhcp detect-dead-server* parameter specifies the number of consecutive failures that could occur before the server is marked as down.
In addition, the **retransmission-timeout** command controls the amount of time between re-tries.

Example

The following command configures the maximum number of times the system re-attempts communication with a DHCP server that is unresponsive to *5*:

```
max-retransmissions 5
```

retransmission-timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the DHCP server.

Product

GGSN, ASN-GW, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

retransmission-timeout *time*

time

Specifies the time that the system waits (in milliseconds) before reattempting communication with the DHCP server. *time* is an integer from 100 through 20000. Default: 10000

Usage

This command works in conjunction with the **max-retransmissions** command to establish a limit on the number of times that communication with a DHCP server is attempted before a failure is logged. This parameter specifies the time between retries.

Example

The following command configures a retry timeout of *1000* milliseconds:

```
retransmission-timeout 1000
```

T1-threshold

Configures the DHCP T1 timer as a percentage of the allocated IP address lease.

Product

GGSN, ASN-GW, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

T1-threshold *percentage*

percentage

Specifies the percentage of the allocated IP address lease time at which the DHCP call-line state is changed to "RENEWING". *percentage* is an integer from 40 through 66. Default: 50

Usage

This command is used to identify the time at which a subscriber must renew their DHCP lease as a percentage of the overall lease time. (Refer to the **lease-duration** command in this chapter for information on configuring the IP address lease period.)
For example, if the lease-duration was configured to have a maximum value of 12000 seconds, and this command is configured to 40%, then the subscriber would enter the RENEWING state after 4800 seconds.

Example

The following command configures the T1 threshold to *40*%:

```
T1-threshold 40
```

T2-threshold

Configures the DHCP T2 timer as a percentage of the allocated IP address lease.

Product

GGSN, ASN-GW, HA, P-GW

Privilege

Security Administrator, Administrator

Syntax

T2-threshold *percentage*

percentage

Specifies the percentage of the allocated IP address lease time at which the DHCP call-line state is changed to "REBINDING". *percentage* is an integer from 67 through 99. Default: 88

Usage

This command is used to identify the time at which a subscriber re-binds their DHCP leased IP address as a percentage of the overall lease time. (Refer to the **lease-duration** command in this chapter for information on configuring the IP address lease period.)
For example, if the lease-duration was configured to have a maximum value of 12000 seconds, and this command is configured to 70%, then the subscriber would enter the REBINDING state after 8400 seconds.

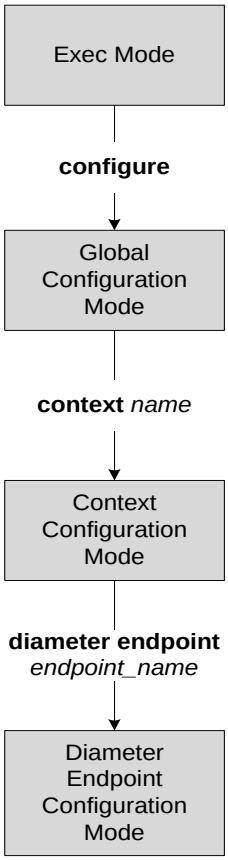
Example

The following command configures the T2 threshold to *70*%:

T2-threshold 70 *70*

Chapter 100
Diameter Endpoint Configuration Mode Commands

Diameter Endpoint Configuration Mode is accessed from the Context Configuration Mode. The base Diameter protocol operation is configured in this mode.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

associate

This command associates/disassociates a Stream Control Transmission Protocol (SCTP) parameter template with the Diameter endpoint.

Product

MME

Privilege

Administrator

Syntax

associate sctp-parameters-template *template_name*

no associate sctp-parameters-template

no

Disassociates an SCTP parameter template with the Diameter endpoint.

sctp-parameters-template *template_name*

Associates a previously created SCTP parameter template with the Diameter endpoint. *template_name* specifies the name for a pre-configured SCTP parameter template. For more information on SCTP parameter templates, refer to the **sctp-param-template** command in the *Global Configuration Mode Commands* chapter.

Usage

Use this command to associate a configured SCTP parameter template with the Diameter endpoint. The SCTP parameter template allows for SCTP timer values to be configured for the interface using the Diameter endpoint configuration. For more information on SCTP parameters, refer to the *SCTP Parameter Template Configuration Mode Commands* chapter.

Important: Only one SCTP parameter template can be associated with the Diameter endpoint configuration. The SCTP parameter template should be configured prior to issuing this command.

Only the following parameters from the template will be associated with the endpoint. When no SCTP parameter template is associated with the endpoint, the following default values are used:
sctp-cookie-life *60000* (default for the parameter template as well)
sctp-max-init-retx *5* (default for the parameter template as well)
sctp-max-path-retx *10* (default in the parameter template is 5)
sctp-rto-initial *3000* (default for the parameter template as well)
sctp-rto-max *60000* (default for the parameter template as well)
sctp-rto-min *1000* (default for the parameter template as well)
sctp-sack-period *200* (default for the parameter template as well)
timeout sctp-heart-beat *30* (default for the parameter template as well)

Example

The following command associates a pre-configured SCTP parameter template called *sctp1* to the Diameter endpoint:

```
associate sctp-parameters-template sctp1
```

cea-timeout

This command configures the Capabilities-Exchange-Answer (CEA) message timeout duration for Diameter sessions.

Product

All

Privilege

Security Administrator, Administrator

Syntax

cea-timeout *timeout*

default cea-timeout

default

Configures this command with the default setting.
Default: 30 seconds

timeout

Specifies the timeout duration (in seconds) to make the system wait for this duration for a CEA message. *timeout* must be an integer from 1 through 120.

Usage

Use this command to configure the CEA timer, i.e., how long to wait for the Capabilities-Exchange-Answer message.

Example

The following command sets the Diameter CEA timeout to *16* seconds:

```
cea-timeout 16
```

connection retry-timeout

This command configures the Diameter Connection Retry Timeout parameter.

Product

All

Privilege

Security Administrator, Administrator

Syntax

connection retry-timeout *timeout*

default connection retry-timeout

default

Configures this command with the default setting.
Default: 30 seconds

timeout

Specifies the connection retry timeout duration in seconds, and must be an integer from 1 through 3600.

Usage

Use this command to configure the Diameter Connection Retry Timeout parameter.

Example

The following command sets the Diameter Connection Retry Timer to *120* seconds:

```
connection retry-timeout 120
```

connection timeout

This command configures the Diameter Connection Timeout parameter.

Product

All

Privilege

Security Administrator, Administrator

Syntax

connection timeout *timeout*

default connection timeout

default

Configures this command with the default setting.
Default: 30 seconds

timeout

Specifies the connection timeout duration (in seconds) as an integer from 1 through 30.

Usage

Use this command to configure the Diameter Connection Timeout parameter.

Example

The following command sets Diameter connection timeout to *16* seconds:

```
connection timeout 16
```

destination-host-avp

This command controls encoding of the Destination-Host AVP in initial/retried requests.

Product

All

Privilege

Security Administrator, Administrator

Syntax

destination-host-avp { session-binding | always | initial-request | retried-request }

default destination-host-avp

default

Configures this command with the default setting. Default: session-binding

session-binding

Includes the Destination-Host AVP when the Diameter session is bound with a host.

always

Includes the Destination-Host AVP in all types of request messages.

initial-request

Includes the Destination-Host AVP in an initial request but not in a retried request.

retried-request

Includes the Destination-Host AVP in a retried request but not in an initial request.

Usage

Use this command to control encoding of the Destination-Host AVP in initial/retried requests.
This command has been introduced in release 12.0, in earlier releases, the Destination-Host AVP is not sent in session-setup/initial request (first message sent on that interface for that subscriber. The message will vary with different interfaces. For example, CCR-Initial for Gy, ACR-start for Rf, and so on). Also, Destination-Host AVP was not sent in retried requests. For example, CCR-Update failed to be responded by server. The message was retransmitted to alternate server.
In both these scenarios, it is not known which server will respond to the initial/retried message, so the Destination-Realm is encoded but not the Destination-Host. Only after a response for this message is received from one of the hosts present in that realm, the session is considered to be BOUND with that server. Any message sent after this binding will have the Destination-Host AVP encoded.
In this release, with this CLI command, if the application has selected one of the servers using application-level commands like the **peer-select** command for credit-control or the **diameter authentication** or **accounting server** command in a AAA group, encoding of this AVP in initial/retried request is configurable.

Example

The following command specifies to include the Destination-Host AVP in initial request but not in retried request:

```
destination-host-avp initial-request
```

device-watchdog-request

This command manages the transport failure algorithm and configures the number of Device Watchdog Requests (DWRs) that will be sent before a connection is closed.

Product

All

Privilege

Security Administrator, Administrator

Syntax

device-watchdog-request max-retries *retry_count*

default device-watchdog-request max-retries

default

Configures this command with the default setting. Default: 1

retry_count

Specifies the maximum number of DWRs, and must be an integer from 1 through 10.

Usage

Use this command to configure the number of DWRs to be sent before closing the connection from a Diameter endpoint.

Example

The following command sets the DWRs to *3*:

```
device-watchdog-request max-retries 3
```

dpa-timeout

This command configures the Disconnect-Peer-Answer (DPA) message timeout duration for Diameter sessions.

Product

All

Privilege

Security Administrator, Administrator

Syntax

dpa-timeout *timeout*

default dpa-timeout

default

Configures this command with the default setting.
Default: 30 seconds

timeout

Specifies the DPA message timeout duration (in seconds) as an integer from 1 through 60.

Usage

Use this command to set the timer for DPA message timeout during Diameter connection session. This makes the system wait for this duration for DPA message.

Example

The following command sets the Diameter DPA timeout to *16* seconds:

```
dpa-timeout 16
```

dscp

This command sets the Differential Services Code Point (DSCP) value in the IP header of the Diameter messages sent from the Diameter endpoint.

Product

All

Privilege

Security Administrator, Administrator

Syntax

dscp { *value* **| af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }**

default dscp

value

Specifies to configure a unique DSCP as an integer in the range of 0 through 63.

af *xx*

Specifies the use of an assured forwarding *xx* per hop behavior (PHB).

be

Specifies the use of best effort forwarding PHB. This is the default.

cs*x*

Specifies the use of class selector *x* per PHB.

ef

Specifies the use of expedited forwarding PHB.

Usage

Use this command to set the DSCP in the IP header of the diameter messages sent from the diameter endpoint. In addition to the recommended PHBs the user may configure their own DSCP as an integer in the range of 0 through 63.

Example

The following command sets the DSCP to *be*:

```
dscp be
```

dynamic-peer-discovery

This command configures the system to dynamically locate peer Diameter servers by means of DNS.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
dynamic-peer-discovery [ protocol { sctp | tcp } ]

{ default | no } dynamic-peer-discovery
```

default

Configures this command with the default setting.
Default: disabled

no

Removes the configuration.

protocol { sctp | tcp }

Configures peer discovery to use a specific protocol. Default: TCP
sctp: Uses Streaming Control Transmission Protocol (SCTP) for peer discovery.
tcp: Uses Transmission Control Protocol (TCP) for peer discovery.

Usage

Use this command to configure the system to dynamically locate peer Diameter servers by means of DNS. Configure the **dynamic-peer-realm** command to locate Diameter servers using Naming Authority Pointer (NAPTR) queries. If the peer realm command is not configured, configuring this command will still allow applications to trigger an NAPTR query on their chosen realms.
The preferred transport protocol is TCP to resolve instances were multiple NAPTR responses with the same priority are received. The one using the TCP transport protocol will be chosen. If the transport protocol is configured through the CLI, then the configured protocol is given preference.
The IP address version will be the same as that of the origin host address configured for the endpoint. For IPv4 endpoints, A-type DNS queries will be sent to resolve Fully Qualified Domain Names (FQDNs). For IPv6 endpoints, AAAA-type queries are sent.

Example

The following command configures the system to dynamically locate peer Diameter servers using SCTP:

```
dynamic-peer-discovery protocol sctp
```

dynamic-peer-failure-retry-count

This command configures the number of times the system will attempt to connect to a dynamically discovered Diameter peer.

Product

All

Privilege

Security Administrator, Administrator

Syntax

dynamic-peer-failure-retry-count *no_of_retries*

default dynamic-peer-failure-retry-count

default

Configures this command with the default setting.
Default: 8

no_of_retries

Specifies the number of retry attempts to connect to a dynamically discovered Diameter peer. The value must be an integer from 0 through 255.

Usage

Use this command to configure the number of times the system attempts to connect to a dynamically discovered Diameter peer.
After the specified number of attempts if the peer is still not open, the peer is moved into blacklist and other peers are tried. The blacklisted peer will be retried after a time period of one hour.

Example

The following command sets the retry attempts to *10*:

```
dynamic-peer-failure-retry 10
```

dynamic-peer-realm

This command configures the name of the realm where peer Diameter servers can be dynamically discovered.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] dynamic-peer-realm *realm_name*

no

Removes the specified dynamic peer realm name from this endpoint configuration.

realm_name

Specifies the name of the peer realm where peer Diameter server are to be dynamically discovered. *realm_name* must be an existing realm, and must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to locate Diameter servers using Naming Authority Pointer (NAPTR) queries. Multiple realms can be configured. Even if the **dynamic-peer-discovery** command is not enabled, the realm configuration(s) will trigger dynamic peer discovery on all diabase instances.

Example

The following command configures a peer realm, used for dynamic peer discovery, with a name of *service-provider.com*:

```
dynamic-peer-realm service-provider.com
```

dynamic-route

This command configures the expiration time for dynamic routes created after a Diameter destination host is reached.

Product

All

Privilege

Security Administrator, Administrator

Syntax

dynamic-route expiry-timeout *value*

default dynamic-route expiry-timeout

default

Configures this command with the default setting. Default: 86400 seconds (1 day)

value

Specifies the time (in seconds) that a dynamic route to a Diameter host will expire. The value must be an integer from 1 through 86400000.

Usage

Use this command to set expiration times for dynamic routes that are set up after a Diameter host has been reached.

Example

The following command sets the dynamic route expiration to *43200* seconds:

```
dynamic-route expiry-timeout 43200
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

load-balancing-algorithm

This command configures the behavior for load balancing Diameters peers in the event of a failure of an active server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

load-balancing-algorithm { highest-weight | lowest-weight-borrowing min-active-servers *number* **}**

default load-balancing-algorithm

default

Configures this command with the default setting.
Default: **highest-weight**

highest-weight

Selects an idle server with the highest weight in failure scenarios. If multiple servers have the same high weight, load balancing is performed among those servers.

lowest-weight-borrowing min-active-servers *number*

Borrows an idle server with the lowest weight and adds it to the group of servers where load balancing is performed. *number* specifies the number of servers that must always be available as active for load balancing. *number* must be an integer from 2 through 4000.

Usage

Use this command to configure the behavior for load balancing Diameter peers in the event of a failure of an active server.

Example

The following command configures the load balancing behavior for Diameter peers to borrowing minimally active servers (lower weight) and maintaining an active server group of *30* servers:

```
load-balancing-algorithm lowest-weight-borrowing min-active-servers 30
```

max-outstanding

This command configures the maximum number of Diameter messages that any application can send to any one peer, while awaiting responses.

Product

All

Privilege

Security Administrator, Administrator

Syntax

max-outstanding *messages*

{ default | no } max-outstanding

no

Disables the maximum outstanding messages configuration.

default

Configures this command with the default setting.
Default: 256

messages

Specifies the maximum outstanding peer transmit window size setting. The input must be an integer from 1 through 4096.

Usage

Use this command to set the unanswered Diameter messages that any application may send to any one peer, while awaiting responses. An application will not send any more Diameter messages to that peer until it has disposed of at least one of those queued messages. It disposes a message by either receiving a valid response or by discarding the message due to no response.

Example

The following command sets the Diameter maximum outstanding messages setting to *1024*:

```
max-outstanding 1024
```

origin address

This command has been deprecated. See the origin host and origin realm commands.

origin host

This command sets the origin host for the Diameter endpoint.

Product

All

Privilege

Security Administrator, Administrator

Syntax

origin host *host_name* **address** *ipv4/ipv6_address* **[port** *port_number* **] [accept-incoming-connections] [address** *ipv4/ipv6_address_secondary* **]**

no origin host *host_name* **address** *ipv4/ipv6_address* **[port** *port_number* **]**

no

Removes the origin host configuration.

origin host *host_name*

Specifies the host name to bind the Diameter endpoint. *host_name* must be the local Diameter host name, and must be an alphanumeric string of 1 through 255 characters.

address *ipv4/ipv6_address*

Specifies the IP address to bind the Diameter endpoint using IPv4 dotted-decimal or IPv6 colon-separated notation. This address must be one of the addresses of a chassis interface configured within the context in which Diameter is configured.

port *port_number*

Specifies the port number for the Diameter endpoint (on inbound connections). The port number must be an integer from 1 through 65535. Default: 3868
Port number in the origin host should be configured only when the chassis is running in server mode, i.e. when **accept-incoming-connections** is configured.
In this case it will open a listening socket on the specified port. For configurations where chassis is operating as a client, port number should not be included. In this case, a random source port will be chosen for outgoing connections. This is applicable for both with or without multi-homing.

Important: Currently if multi-homing is configured, then the specified port is used instead of randomly chosen port. This is done so that application knows which port is used by the kernel as it will have to use the same port while adding/removing IP address from the association. Nevertheless, configuring port number in origin host for client mode is not supported.

accept-incoming-connections

Accepts inbound connection requests for the specified host.

address *ipv4/ipv6_address_secondary*

Specifies the secondary bind address for the Diameter endpoint in IPv4 dotted-decimal or IPv6 colon-separated notation. This address must be one of the addresses of a chassis interface configured within the context in which Diameter is configured.

Usage

Use this command to set the bind address for the Diameter endpoint.
Diameter agent on the chassis listens to standard TCP port 3868 and also supports the acceptance of any incoming TCP connection from external server.
The command **origin host** *host-name* must be entered exactly once. Alternatively, the **origin host** *host-name* **address** *ipv4/ipv6_address* **[port** *port_number* **]** command may be entered one or more times. The host names should be unique across all endpoints within the system. The host names and address values or address/port combinations should be unique across all endpoints within the system.

Example

The following command sets the origin host name to *test* and the IP address to *10.1.1.1*:

```
origin host test address 10.1.1.1
```

origin realm

This command configures the realm to use in conjunction with the origin host.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] origin realm *realm_name*

no

Removes the origin realm configuration.

realm_name

Specifies the realm to bind the Diameter endpoint. The *realm_name* must be an alphanumeric string of 1 through 127 characters. The realm is the Diameter identity. The originator's realm must be present in all Diameter messages. The origin realm can typically be a company or service name.

Usage

Use this command to set the realm for the Diameter endpoint.
Diameter agent on the chassis listens to standard TCP port 3868 and also supports the acceptance of any incoming TCP connection from external server.

Example

The following command sets the origin realm to *companyx*:

```
origin realm companyx
```

peer

This command specifies a peer address for the Diameter endpoint.

Product

All

Privilege

Security Administrator, Administrator

Syntax

peer [*] *peer_name* **[*] [realm** *realm_name* **] { address** *ipv4/ipv6_address* **[[port** *port_number* **] [connect-on-application-access] [send-dpr-before-disconnect disconnect-cause** *disconnect_cause* **] [sctp]] + | fqdn** *fqdn* **[[port** *port_number* **] [send-dpr-before-disconnect disconnect-cause** *disconnect_cause* **]] }**

no peer *peer_name* **[realm** *realm_name* **]**

no

Removes the specified peer configuration.

[*] *peer_name* **[*]**

Specifies the peer's name as an alphanumeric string of 1 through 63 characters that allows punctuation characters.
The Diameter server endpoint can now be a wildcarded peer name (with * as a valid wildcard character). Client peers which satisfy the wild-carded pattern are treated as valid peers and the connection will be accepted. The wildcarded token indicates that the peer name is wildcarded and any '*' in the preceding string is treated as a wildcard.

realm *realm_name*

Specifies the realm of this peer as an alphanumeric string of 1 through 127 characters. The realm name can be a company or service name.

address *ipv4/ipv6_address*

Specifies the Diameter peer IP address in IPv4 dotted-decimal or IPv6 colon-separated notation. This address must be the IP address of the device with which the chassis is communicating.

fqdn *fqdn*

Specifies the Diameter peer FQDN as an alphanumeric string of 1 through 127 characters.

port *port_number*

Specifies the port number for this Diameter peer. The port number must be an integer from 1 through 65535.

connect-on-application-access

Activates peer on first application access.

send-dpr-before-disconnect

Sends Disconnect-Peer-Request (DPR).

disconnect-cause

Sends Disconnect-Peer-Request to the specified peer with the specified disconnect reason. The disconnect cause must be an integer from 0 through 2, for one of the following:

- REBOOTING(0)
- BUSY(1)
- DO_NOT_WANT_TO_TALK_TO_YOU(2)

sctp

Uses Stream Control Transmission Protocol (SCTP) for this peer.

+

Indicates that more than one of the previous keywords can be entered within a single command.

Usage

Use this command to add a peer to the Diameter endpoint.
If the Diameter server side endpoint is catering to multiple peers, there has to be an entry for each peer in the peer list for that endpoint.
In cases where the client like GGSN does not use a diameter proxy, the peer list can be as large as the number of session managers on a GGSN. This might lead to a very complex configuration at the Diameter server endpoint.
To simplify the configurations, the Diameter server endpoint accepts a wildcarded peer name (with * as a valid wildcard character).
The client peers which satisfy the wild-carded pattern are treated as valid peers and the connection will be accepted. The new token ‘wildcarded*’ indicates that the peer name is wildcarded and any ‘*’ in the preceding string should be treated as a wildcard.
For example, if the peer name is prefixed and suffixed with *ggsn* (* wildcard character) and an exact match is not found for the peer name portions peers like *0001-sessmgr.ggsn-gx*, *0002-sessmgr.ggsn-gx*, will be treated as valid peers at the Diameter server endpoint.

Example

The following command adds the peer named *test* with IP address *10.1.1.1* using port *126*:

```
peer test address 10.1.1.1 port 126
```

response-timeout

This command configures the Response Timeout parameter. Response timeout specifies the maximum allowed response time for request messages sent from Diameter applications to Diameter server. On failure of reception of response for those request message within this specified time, this will be handled as failure by the corresponding applications and appropriate failure action will be initiated.

Product

All

Privilege

Security Administrator, Administrator

Syntax

response-timeout *timeout*

default response-timeout

default

Configures this command with the default setting.
Default: 60 seconds

timeout

Specifies the response timeout duration in seconds, and must be an integer from 1 through 300.

Usage

Use this command to configure the Response Timeout parameter.

Example

The following command sets the response timeout to *100* seconds:

```
response-timeout 100
```

route-entry

This command creates an entry in the route table for Diameter peer.

Product

All

Privilege

Security Administrator, Administrator

Syntax

route-entry { [host *host_name* **] [peer** *peer_id* **[weight** *priority* **]] [realm** *realm_name* **[application credit-control peer** *peer_id* **] [weight** *value* **] | peer** *peer_id* **[weight** *value* **]] }**

no route-entry { [host *host_name* **] [peer** *peer_id* **] [realm** *realm_name* **{ application credit-control peer** *peer_id* **| peer** *peer_id* **}] }**

no

Disables the specified route-entry table configuration.

host *host_name*

Specifies the Diameter server's host name as an alphanumeric string of 1 through 63 characters.

realm *realm_name*

Specifies the realm name as an alphanumeric string of 1 through 127 characters. The realm may typically be a company or service name.

application credit-control

Specifies the credit control application — DCCA or RADIUS.

peer *peer_id*

Specifies the peer ID of the Diameter endpoint route as an alphanumeric string of 1 through 63 characters.

weight *priority*

Specifies the priority for a peer in the route table as an integer from 0 through 255. Default: 10
The peer with the highest weight is used. If multiple peers have the highest weight, selection is by round-robin mechanism.

Usage

Use this command to create a route table for Diameter application.
When a Diameter client starts to establish a session with a realm/application, the system searches the route table for the best match. If an entry has no host specified, the entry is considered to match the requested value. Similarly, if an entry has no realm or application specified, the entry is considered to match any such requested value. The best match algorithm is to prefer specific matches for whatever was requested, either realm/application or host/realm/application. If there are no such matches, then system looks for route table entries that have wildcards.

Example

The following command creates a route entry with the host name *dcca_host1* and peer ID *dcca_peer* with priority weight of *10*:

```
route-entry host dcca_host1 peer dcca_peer weight 10
```

route-failure

This command controls what action is performed for the route table after failure or recovery after failure.

Product

All

Privilege

Security Administrator, Administrator

Syntax

route-failure { deadtime *seconds* **| recovery-threshold percent** *percentage* **| result-code** *result_code* **| threshold** *counter* **}**

default route-failure { deadtime | recovery-threshold | threshold }

no route-failure result-code *result_code*

no

Disables the route-failure configuration.

default

Configures the default setting for the specified parameter.

deadtime *seconds*

Specifies the time duration (in seconds) for which the system keeps the route in FAILED status. When this time expires, the system changes the status to AVAILABLE.
seconds must be an integer from 1 through 86400. Default: 60

recovery-threshold percent *percentage*

Specifies the percentage value at which the failure counter is reset when provisionally changing the status from FAILED to AVAILABLE.
For example, if a failure counter of 16 caused the status to change to FAILED. After the configured deadtime expires, the status changes to AVAILABLE. If this keyword is configured with 75 percent, the failure counter will be reset to 12 (75 percent of 16).
percentage must be an integer from 1 through 99. Default: 90

result-code *result_code*

Configures which answer messages are to be treated as failures, in addition to requests that time out. Up to 16 different result codes can be specified.
result_code must be an integer from 0 through 4294967295.

threshold *counter*

Configures the number of errors that causes the status to become FAILED. The counter value must be an integer from 0 through 4294967295. Default: 16
The error counter begins at zero, and whenever there is a good response it decrements (but not below zero) or increments (but not above this threshold).

Usage

Use this command to control how failure/recovery is performed for the route table. After a session is established, it is possible for the session to encounter errors or Diameter redirection messages that cause the Diameter protocol to re-use the route table to switch to a different route.
Each Diameter client within the chassis maintains counters relating to the status of each of its connections to different hosts (when the destination is realm/application without a specific host, the host name is kept as “”, i.e., blank).
Moreover, those counters are further divided according to which peer is used to reach each host. Each Diameter client maintains a status of each peer-to-host combination. Under normal good conditions the status will be AVAILABLE, while error conditions might cause the status to be FAILED.
Only combinations that are AVAILABLE will be used. If none are AVAILABLE, then system attempts the secondary peer if failover is configured and system can find an AVAILABLE combination there. If nothing is AVAILABLE, the system uses a FAILED combination.

Example

The following command configures the time duration for route failure to *90* seconds:

```
route-failure deadtime 90
```

server-mode

This command configures the Diameter endpoint to establish the system as the server side endpoint of the connection.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
server-mode [ demux-mode ]
```

demux-mode

Specifies that the Diameter proxy is to use the demux manager to identify the appropriate session manager. If this keyword is not enabled, the proxy will route the request directly to a session manager.

Usage

Use this command to configure the Diameter endpoint to establish this system as the server side endpoint of the connection. When the Diameter proxy receives an incoming request, the proxy identifies the endpoint for the request. If the system is in client mode, the proxy extracts the instance ID of the session manager which serves as the session-ID of the request. If this command is enabled, the extraction of the instance ID is disabled.

Example

The following command sets the system as the server side of the Diameter endpoint and instructs the Diameter proxy to use the demux manager to identify the appropriate session manager where the request is to be routed:

```
server-mode demux-mode
```

tls

This command enables/disables the Transport Layer Security (TLS) support between a Diameter client and Diameter server node.

Product

All

Privilege

Security Administrator, Administrator

Syntax

tls { certificate *certificate* **| password** *password* **| privatekey** *private_key* **}**

default tls

default

Disables the TLS support at Diameter endpoint.

certificate *certificate*

Specifies the certificate for TLS support. The certificate must appear encrypted, and must be an alphanumeric string of 700 through 900 characters.

password *password*

Specifies the password for TLS support. The password must be encrypted, and must be an alphanumeric string of 6 through 50 characters.

privatekey *private_key*

Specifies the private key for TLS support. The private key must be encrypted, and must be an alphanumeric string of 900 through 1500 characters.

Usage

Use this command to configure TLS support between a Diameter client and Diameter server node. By default, TLS is disabled.

Important: Both the Diameter client and server must be configured with TLS enabled or TLS disabled; otherwise, the Diameter connection will be rejected.

Example

The following commands enable the TLS between a Diameter client and Diameter server node:

```
tls certificate "-----BEGIN CERTIFICATE-----
\nMIICGDCCAYECAgEBMA0GCSqGSIb3DQEBBAUAMFcxCzAJBgNVBAYTAlVTMRMwEQYD\nVQQKE
wpSVEZNLCBJbmMuMRkwFwYDVQQLExBXaWRnZXRzIERpdmlzaW9uMRgwFgYD\nVQQDEw9UZXN0
IENBMjAwMTA1MTcwHhcNMDEwNTE3MTYxMDU5WhcNMDQwMzA2MTYx\nMDU5WjBRMQswCQYDVQQ
GEwJVUzETMBEGA1UEChMKUlRGTSwgSW5jLjEZMBcGA1UE\nCxMQV2lkZ2V0cyBEaXZpc2lvbj
ESMBAGA1UEAxMJbG9jYWxob3N0MIGfMA0GCSqG\nSIb3DQEBAQUAA4GNADCBiQKBgQCiWhMjN
```

```
OPlPLNW4DJFBiL2fFEIkHuRor0pKw25\nJ0ZYHW93lHQ4yxA6afQr99ayRjMY0D26pH41f0qj
DgO4OXskBsaYOFzapSZtQMbT\n97OCZ7aHtK8z0ZGNW/cslu+1oOLomgRxJomIFgW1RyUUkQP
1n0hemtUdCLOLlO7Q\nCPqZLQIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAIumUwl1OoWuyN2xfo
BHYAs+lRLY\nKmFLoI5+iMcGxWIsksmA+b0FLRAN43wmhPnums8eXgYbDCrKLv2xWcvKDP3mp
s7m\nAMivwtu/eFpYz6J8Mo1fsV4Ys08A/uPXkT23jyKo2hMu8mywkqXCXYF2e+7pEeBr\nds
bmkWK5NgoMl8eM\n-----END CERTIFICATE-----\n"

tls privatekey BEGIN RSA PRIVATE KEY-----\nProc-Type: 4,ENCRYPTED\nDEK-
Info: DES-EDE3-
CBC,5772A2A7BE34B611\n\n1yJ+xAn4MudcIfXXy7ElYngJ9EohIh8yvcyVLmE4kVd0xeaL/
Bqhvk25BjYCK5d9\nk1K8cjgnKEBjbC++0xtJxFSbUhwoKTLwn+sBoJDcFzMKkmJXXDbSTOaN
r1sVwiAR\nSnB4lhUcHguYoV5zlRJn53ft7t1mjB6RwGH+d1Zx6t95OqM1lnKqwekwmotVAWH
j\nncu3N8qhmoPMppmzEv0fOo2/pK2WohcJykSeN5zBrZCUxoO0NBNEZkFUcVjR+KsA\n1ZeI
1mU60szqg+AoU/XtFcow8RtG1QZKQbbXzyfbwaG+6LqkHaWYKHQEI1546yWK\nus1HJ734uUk
ZoyyyazG6PiGCYV2u/aY0i3qdmyDqTvmVIvve7E4glBrtDS9h7D40\nnPShIvOatoPzIK4Y0Q
SvrI3G1vTsIZT3IOZto4AWuOkLNfYS2ce7prOreF0KjhV0\n3tggw9pHdDmTjHTiIkXqheZxZ
7TVu+pddZW+CuB62I8lCBGPW7os1f21e3eOD/oY\nYPCI44aJvgP+zUORuZBWqaSJ0AAIuVW9
S83Yzkz/tlSFHViOebyd8Cug4TlxK1VI\nq6hbSafh4C8ma7YzlvqjMzqFifcIolcbx+1A6ot
0UiayJTUra4d6Uc4Rbc9RIiG0\njfDWC6aii9YkAgRl9WqSd31yASge/HDqVXFwR48qdlYQ57
rcHviqxyrwRDnfw/lX\nMf6LPiDKEco4MKej7SR2kK2c2AgxUzpGZeAY6ePyhxbdhA0eY21nD
eFd/RbwSc5s\neTiCCMr41OB4hfBFXKDKqsM3K7klhoz6D5WsgE6u3lDoTdz76xOSTg==\n--
---END RSA PRIVATE KEY-----\n"

tls password TLSpassword_3B167E
```

use-proxy

This command enables/disables Diameter proxy for the Diameter endpoint. By default this command is disabled.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
use-proxy [ server-mode [ demux-mode ] ]

no use-proxy
```

no

Disables Diameter proxy for the current endpoint.
This command at endpoint level will equip an application to use Diameter proxy to route all its messages to an external peer.

server-mode

Specifies that the Diameter endpoint to establish the Diameter proxy as the server side endpoint of the connection.

demux-mode

Specifies that the Diameter endpoint to establish the Diameter proxy to use the Demux manager to identify the appropriate session manager. If this keyword is not enabled, the proxy will route the request directly to a session manager.
IPCF uses BindMux to identify the appropriate session manager.

Usage

Use this command to establish a Diameter proxy to route all its messages to an external peer. The proxy acts as an application gateway for Diameter. It gets the configuration information at process startup and decides which Diameter peer has to be contacted for each application. It establishes the peer connection upon finding no peer connection already exists.
IPCF uses Bindmux as a Demux manager to help distribute new incoming sessions across available Sessmgrs on the system.
All the incoming Diameter requests/responses land on Diamproxy. Diamproxy checks if a Sessmgr is already serving this session based on parameters like session-id and peer-id of the request/response.
If no Sessmgr is allocated to the request and the Demux mode is ON, the DiamProxy forwards the new request to Demux/Bindmux for sessmgr allocation. Demux/Bindmux has updated information about the load on all the Sessmgrs and assigns the optimal Sessmgr to the Diameter session. Once a Sessmgr is allocated for the session, a mapping of session-id to Sessmgr is added at Diamproxy. All further requests for this session will be directly routed to Sessmgr.
Each proxy task will automatically select one of the host names configured with the **origin host** command. Multiple proxy tasks will not use the same host names, so there should be at least as many host names as proxy tasks. Otherwise, some proxy tasks will not be able to perform Diameter functionality. The

chassis automatically selects which proxy tasks are used by which managers (i.e., ACSMgrs, Sessmgrs), without verifying whether the proxy task is able to perform Diameter functionality.
To be able to run this command, the Diameter proxy must be enabled. In the *Global Configuration Mode Commands* chapter, see the description of the **require diameter-proxy** command.

Example

The following command enables Diameter proxy for the current endpoint:

```
use-proxy
```

The following command disables Diameter proxy for the current endpoint:

```
no use-proxy
```

vsa-support

This command allows DIABASE to use vendor IDs configured in the dictionary for negotiation of the Diameter peers' capabilities regardless of the supported vendor IDs received in Capabilities-Exchange-Answer (CEA) messages.

Product

GGSN, PDSN

Privilege

Security Administrator, Administrator

Syntax

```
vsa-support { all-from-dictionary | negotiated-vendor-ids }

default vsa-support
```

default

Configures this command with the default setting.
Default: **negotiated-vendor-ids**

all-from-dictionary

Allows DIABASE to use the vendor IDs from the dictionary as indicated in the Capabilities-Exchange-Request (CER) messages from Diameter peers.

negotiated-vendor-ids

Allows DIABASE to use the supported vendor IDs satisfying capability negotiation.

Usage

Use this command to set DIABASE to use the vendor IDs from the dictionary or use the vendor IDs satisfying the capabilities negotiation.

Example

The following command enables DIABASE to use the vendor IDs specified in the dictionary:

```
vsa-support all-from-dictionary
```

watchdog-timeout

This command configures the Watchdog Timeout parameter.

Product

All

Privilege

Security Administrator, Administrator

Syntax

watchdog-timeout *timeout*

{ default | no } watchdog-timeout

no

Disables the watchdog timeout configuration.

default

Configures this command with the default setting.
Default: 30 seconds

timeout

Specifies the timeout duration (in seconds) as an integer from 6 through 30.

Usage

Use this command to configure the Watchdog Timeout parameter for the Diameter endpoint. If this timer expires before getting a response from the destination, other route to the same destination is tried, as long as the retry count setting has not exceeded (see the device-watchdog-request CLI command) and as long as the response timer has not expired (see the response-timeout CLI command).

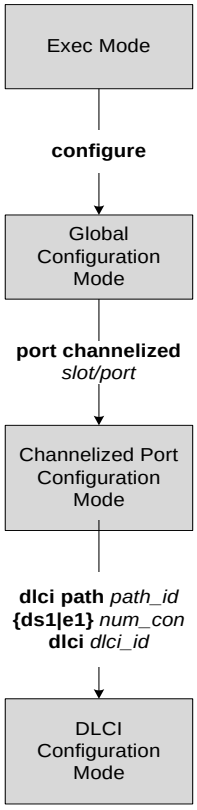
Example

The following command sets the watchdog timeout setting to *15* seconds:

```
watchdog-timeout 15
```

Chapter 101
DLCI Configuration Mode Commands

The DLCI configuration mode provides the commands to configure, bind and manage the DLCI associated with a specific port defined in the parent configuration mode, Channelized Port configuration mode.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

bind link

This command configures an association (binds) between an IP interface or a pre-configured routing SS7/Frame Relay link and the specific port being configured with the Channelized Port configuration commands.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] bind link peer-nsei *nse_id* **ns-vci** *ns-vc_id*

peer-nsei *nse_id*

Defines the end-point network service entity identifier (NSEI). The NSEI must be an integer from 0 to 65535.

ns-vc-id *ns-vc_id*

Defines the network service virtual circuit identifier (NSVCI). The NSVCI must be an integer from 0 to 65535.

no

Deletes the bind configuration from the Operator Policy.

Usage

Bind this port to network service entity 2 and network service VC 234.

Example

```
bind link peer-nsei 2 ns-vci 234
```

end

Exits this sub-configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Change the mode and return to the Exec mode.

exit

Exits the this sub-configuration mode and returns to the parent configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the previous configuration mode.

shaping

Defines egress traffic shaping to control flow for this DLCI.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

shaping *type*

default shaping

shaping *type*

The following types of shaping provide flow management:

- **cir:** Commited Info Rate
- **cir-eir:** Commited Info Rate with Excess Rate
- **ppr:** Peak Packet Rate
- **wfq:** Weighted Fair Queuing

default

Resets the DLCI configuration to the system default.

Usage

Use this command to identify the type of signal shaping to be used on the DLCI.

Example

shaping *cir*

shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, this command with the **no** keyword enables the port.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] shutdown
```

no

Enables the port's administrative state. When omitted the card is shutdown (removed from service).

Usage

Shut down a port prior to re-cabling and/or other maintenance activities.
This command with the **no** keyword is required to bring a port into service.

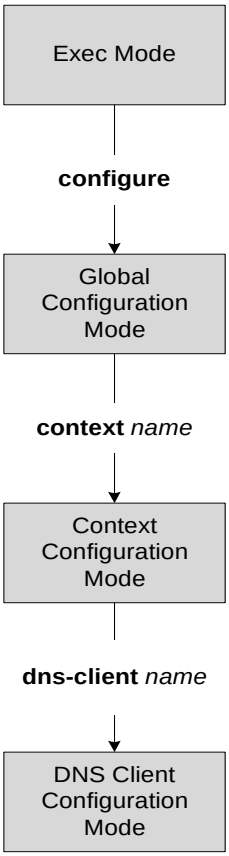
Example

Use the following command to disable the DLCI:

```
no shutdown
```

Chapter 102
DNS Client Configuration Mode Commands

The DNS Client Configuration Mode is used to manage the system's DNS interface and caching parameters.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

bind

Binds the DNS client to a pre-configured logical IP interface.

Product

MME, SCM, SGSN

Privilege

Security Administrator, Administrator

Syntax

bind { address *ip_address* **[port** *number* **] | query-over-gtp }**

no bind address

no

Removes the binding of the client to a specified interface.

bind address *ip_address*

Specifies the IP address of the interface to which the DNS client is being bound in IPv4 dotted-decimal notation.

bind port *number*

Specifies the UDP port number of the interface to which the DNS client is being bound as an integer from 1 to 65535. Default: 6011

bind query-over-gtp

Specifies that DNS client query is to be performed over GTP.

Usage

Use this command to associated the client with a specific logical IP address.

Example

The following command binds the DNS client to a logical interface with an IP address of *10.2.3.4* and a port number of *6000*:

```
bind address 10.2.3.4 port 6000
```

cache algorithm

Configures the method of use for the DNS VPN and session cache.

Product

MME, SCM, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
cache algorithm { central | local } { FIFO | LRU | LFU }

default cache algorithm { central | local }
```

default

Sets the DNS VPN and session cache method to default setting.

central | local

central: Specifies the central proclet (VPN manager)
local: Specifies the local proclet (session manager)

FIFO | LRU | LFU

FIFO: First in first out. This is the default setting for the central proclet.
LRU: Least recently used. This is the default value for the local proclet.
LFU: Least frequently used.

Usage

Use this command to configure the method by which entries are added and removed from the DNS cache.

Example

The following command configures the cache algorithm for the central proclet to least frequently used (LFU):

```
cache algorithm central lfu
```

cache size

Configures the maximum number of entries allowed in the DNS cache.

Product

MME, SCM, SGSN

Privilege

Security Administrator, Administrator

Syntax

cache size { central | local } *max_size*

default cache size { central | local }

default

Sets the maximum number of entries allowed in the DNS cache to default setting.

{ central | local } *max_size*

central *max_size*: Specifies the maximum number of entries allowed in the central proclet cache as an integer from 100 through 65535. Default: 50000.
local *max_size*: Specifies the maximum number of entries allowed in the local proclet cache as an integer from 100 through 65535. Default: 1000.

Usage

Use this command to configure the maximum number of entries allowed in the DNS cache.

Example

The following command configures the cache size of the central proclet to *20000*:

```
cache size central 20000
```

cache ttl

Configures the DNS cache time to live (TTL) for positive and negative responses.

Product

MME, SCM, SGSN

Privilege

Security Administrator, Administrator

Syntax

cache ttl { negative | positive } *seconds*

default cache ttl { negative | positive }

no cache [ttl { negative | positive }]

no

Disables any or all configured DNS cache parameters.

default

Sets the DNS cache time to live for positive and negative responses to the default setting.

{ negative | positive } *seconds*

negative *seconds*: Specifies the time to live for negative responses as an integer from 60 through 86400. Default: 60.
positive *seconds*: Specifies the time to live for positive responses. as an integer from 60 through 86400. Default: 86400 (1 day).

Usage

Use this command to adjust the DNS cache time to live.

Example

The following commands set the TTL DNS cache to *90* seconds for negative responses and *43200* seconds for positive responses:

```
cache ttl negative 90

cache ttl positive 43200
```

case-sensitive

Configures the case sensitivity requirement for responses to DNS requests.

Product

MME, SCM, SGSN

Privilege

Administrator

Syntax

```
[ default | no ] case-sensitive response
```

default

Returns the command to its default setting of disabled.

no

Disables the requirement for case sensitivity in DNS responses.

case-sensitive response

Enables the requirement for case sensitivity in DNS responses.

Usage

Use this command to require case sensitivity (identical case usage between request and response) on all responses to DNS request messages.

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

resolver

Configures the number of DNS query retries and the retransmission interval once the response timer expires.

Product

MME, SGSN

Privilege

Security Administrator, Administrator

Syntax

resolver { number-of-retries *retries* **| retransmission-interval** *time* **}**

default { number-of-retries | retransmission-interval }

default

Resets the specified resolver configuration to the default.

number-of-retries *retries*

Configures the number of DNS query retries on DNS response timeout as an integer from 0 through 4. Default: 2.

retransmission-interval *time*

Configures the initial retransmission interval (in seconds) for retransmission after the DNS response timeout as an integer from 2 to 5. Default is 3 seconds. The retransmission interval doubles after each retry when only one server is configured. In case both primary and secondary servers are configured, the retransmission time is doubled for the last retry.

Usage

Set the DNS retransmission retries or the retransmission interval. Issue the command twice to configure both parameters, one-at-a-time.

Example

The following command sets the DNS resolver retries to *4*:

```
resolver number-of-retries 4
```

round-robin answers

Configures the DNS client to return the DNS results in round-robin fashion if multiple results are available for a DNS query.

Product

MME, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] round-robin-answers
```

no

Removes the configured round robin method for DNS answer.

default

Disables the round robin method for DNS answer.

round-robin-answers

Enables the round robin method for DNS answer.

Usage

Use this command to configure the DNS client to return the DNS results in round-robin fashion if multiple results are available for a DNS query.

Example

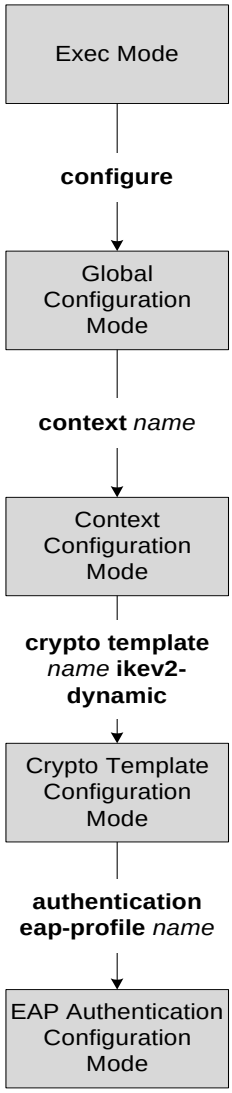
The following command configures the DNS client to use round robin method for DNS query answers:

```
default ] round-robin-answers
```

Chapter 103
EAP Authentication Configuration Mode Commands

The EAP Authentication Configuration Mode is used to configure the Extensible Authentication Protocol (EAP) authentication methods for the crypto template.

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).



eap-aka

Configures shared key values for the Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) authentication method used by subscribers using this crypto template.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

eap-aka { encrypted key *hex* **| key** *hex* **}**

encrypted key *hex*

Specifies that the shared key is to be encrypted as a 16-character alphanumeric string or a hexadecimal number beginning with “0x”.

key *hex*

Specifies that the shared key is to be transmitted in clear text as a 16-character alphanumeric string or a hexadecimal number beginning with “0x”.

Usage

Use this command to set shared key parameters for subscribers using the EAP-AKA authentication method.

Example

The following command configures a clear-text shared key value for the EAP-AKA method:

```
eap-aka key aa11223344556677
```

eap-gtc

Configures shared key values for the EAP-GTC authentication method used by subscribers using this crypto template.

Product

PDIF, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

eap-gtc { encrypted key *value* **| key** *value* **}**

encrypted key *value*

Specifies that the shared key is to be encrypted as a 16-character alphanumeric string.

key *value*

Specifies that the shared key is to be transmitted in clear text as a 16-character alphanumeric string.

Usage

Use this command to set shared key parameters for subscribers using the EAP-GTC authentication method.

Example

The following command configures a clear-text shared key value for the EAP-GTC method:

```
eap-GTC key aa11223344556677
```

eap-md5

Configures shared key values for the EAP-MD5 authentication method used by subscribers using this crypto template.

Product

PDIF, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

```
eap-md5 { encrypted key value | key value }
```

encrypted key *value*

Specifies that the shared key is to be encrypted as a 16-character alphanumeric string.

key *value*

Specifies that the shared key is to be transmitted in clear text as a 16-character alphanumeric string.

Usage

Use this command to set shared key parameters for subscribers using the EAP-MD5 authentication method.

Example

The following command configures a clear-text shared key value for the EAP-MD5 method:

```
eap-md5 key aa11223344556677
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

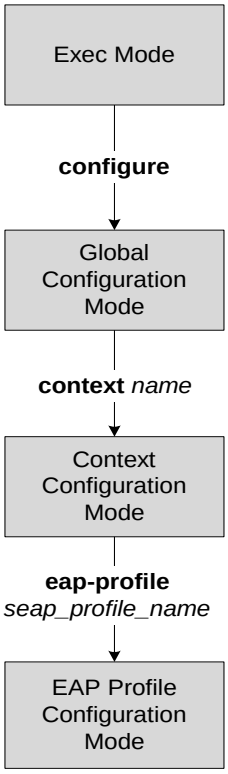
```
exit
```

Usage

Use this command to return to the parent configuration mode.

Chapter 104
EAP Configuration Mode Commands

The EAP Configuration Mode is used to configure parameters comprising an Extensible Authentication Protocol (EAP) used to support authentication on the system.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

max-retry

Configures the maximum number of times the system will retry communicating with another EAP device.

Product

PDIF, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

max-retry *num*

default max-retry

max-retry *num*

Specifies the number of times to retry EAP communication with another device as an integer from 1 to 65535. Default: 16

Usage

Use this command to set a maximum retry number for communicating with other EAP devices.

Example

The following command sets the maximum number of retries to *50*:

```
max-retry 50
```

mode

Configures the system as one of three types of EAP devices: authenticator pass-through, authenticator server, or peer.

Product

PDIF, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

```
mode { authenticator-pass-through | authenticator-server | peer }

default mode
```

default

Configures the default mode of Authenticator-pass-through.

authenticator-pass-through

Configures the system as an authenticator pass-through allowing EAP authentication to be performed by another server.
This is the default setting for this command.

authenticator-server

Configures the system as an authenticator server. This allows the system to respond to EAP requests.

peer

Configures the system as a peer device requiring it to make EAP requests of another server or pass-through device.

Usage

Use this command to configure the system to perform as one of three types of EAP devices and configure settings in an EAP mode.
EAP Mode Configuration Mode commands are defined in the EAP Mode Configuration Mode Commands chapter.

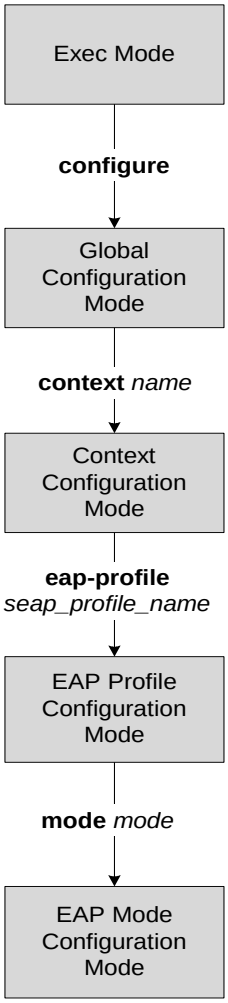
Example

The following command configures the system to perform as an authenticator pass-through:

```
mode authenticator-pass-through
```

Chapter 105
EAP Mode Configuration Mode Commands

The EAP Mode Configuration Mode is used to configure the Extensible Authentication Protocol (EAP) authentication method supported by the system.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

method

Configures the EAP method used for authentication.

Product

PDIF, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

method { eap-aka | eap-gtc | eap-md5 } [priority *num* **]**

eap-aka | eap-gtc | eap-md5

Specifies one of the following methods:

- **eap-aka**: Specifies that the EAP-AKA method is to be used for authentication.
- **eap-gtc**: Specifies that the EAP-GTC method is to be used for authentication.
- **eap-md5**: Specifies that the EAP-MD5 method is to be used for authentication.

priority *num*

Specifies a priority order for a specific EAP authentication method an integer from 1 though 65535.

Usage

Use this command to specify the EAP authentication method(s) to use and to place multiple methods in priority order.

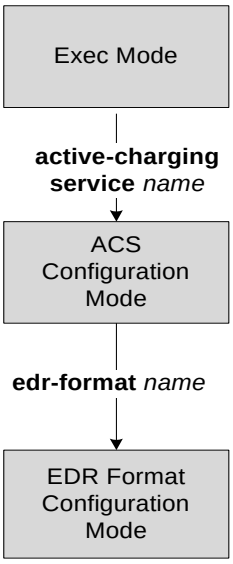
Example

The following command sets EAP-AKA as one of the EAP authentication methods and places it as priority of 3:

```
method eap-aka priority 3
```

Chapter 106
EDR Format Configuration Mode Commands

The EDR Format Configuration Mode enables configuring Event Data Record (EDR) formats.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

attribute

This command allows you to specify the fields and their order in EDRs.

Product

All

Privilege

Security Administrator, Administrator

Syntax

attribute *attribute* **{ [format { MM/DD/YY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds }] [localtime] | [{ ip | tcp } { bytes | pkts } { downlink | uplink }] priority** *priority* **}**

no attribute *attribute* **[{ ip | tcp } { bytes | pkts } { downlink | uplink }] [priority** *priority* **]**

no

If added previously, removes the specified attribute from the EDR format.

attribute

Specifies the attribute.
attribute must be one of the following:

Attributes	Description
radius-called-station-id	This attribute reports the Called Station ID of the mobile handling the flow.
radius-calling-station-id	This attribute reports the Calling Station ID of the mobile handling the flow.
radius-fa-nas-identifier	This attribute reports the RADIUS NAS identifier of Foreign Agent (FA).
radius-fa-nas-ip-address	This attribute reports the RADIUS IP address of Foreign Agent (FA).
radius-nas-identifier	This attribute reports the RADIUS NAS identifier.
radius-nas-ip-address	This attribute reports the RADIUS NAS IP address.
radius-user-name	This attribute reports the user name associated with the flow.
sn-3gpp2-always-on	This option has been deprecated. To configure this attribute see the rule-variable command.
sn-3gpp2-bsid	This option has been deprecated. To configure this attribute see the rule-variable command.
sn-3gpp2-esn	This option has been deprecated. To configure this attribute see the rule-variable command.

Attributes	Description
sn-3gpp2-ip-qos	This option has been deprecated. To configure this attribute see the rule-variable command.
sn-3gpp2-ip-technology	This option has been deprecated. To configure this attribute see the rule-variable command.
sn-3gpp2-release-indicator	This option has been deprecated. To configure this attribute see the rule-variable command.
sn-3gpp2-service-option	This option has been deprecated. To configure this attribute see the rule-variable command.
sn-3gpp2-session-begin	This option has been deprecated. To configure this attribute see the rule-variable command.
sn-3gpp2-session-continue	This option has been deprecated. To configure this attribute see the rule-variable command.
sn-acct-session-id	This attribute reports the unique session identifier for accounting.

Attributes	Description
sn-app-protocol	This attribute reports the application protocol for the flow. A value indicating the protocol, such as one of the following: • ACS_PROTO_UNKNOWN = 0 • ACS_PROTO_GTP = 1 • ACS_PROTO_IP = 2 • ACS_PROTO_TCP = 3 • ACS_PROTO_UDP = 4 • ACS_PROTO_HTTP = 5 • ACS_PROTO_HTTPS = 6 • ACS_PROTO_FTP = 7 • ACS_PROTO_FTP_CONTROL = 8 • ACS_PROTO_FTP_DATA = 9 • ACS_PROTO_WTP = 10 • ACS_PROTO_WSP = 11 • ACS_PROTO_WTP_WSP_CONNECTION_ORIENTED = 12 • ACS_PROTO_WSP_CONNECTION_LESS = 13 • ACS_PROTO_DNS = 14 • ACS_PROTO_ICMP = 15 • ACS_PROTO_POP3 = 16 • ACS_PROTO_SIP = 17 • ACS_PROTO_SDP = 18 • ACS_PROTO_SMTP = 19 • ACS_PROTO_EMAIL = 20 • ACS_PROTO_MMS = 21 • ACS_PROTO_FILE_TRANSFER = 22 • ACS_PROTO_WWW = 23 • ACS_PROTO_RTP = 24 • ACS_PROTO_RTSP = 25 • ACS_PROTO_IMAP = 26 • ACS_PROTO_FLOW = 27 • ACS_PROTO_CCA = 28 • ACS_PROTO_P2P = 29 • ACS_PROTO_RTCP = 30 • ACS_PROTO_ICMPV6 = 31 • ACS_PROTO_TFTP = 32 • ACS_PROTO_PPTP = 33

Attributes	Description
	• ACS_PROTO_GREv1 = 34 • ACS_PROTO_PPTP_GRE = 35 • ACS_PROTO_SIP_ADV = 36 • ACS_PROTO_SIP_BASIC_ADV = 37 • ACS_PROTO_H323 = 38
sn-cf-category-classification-used	For Category-based Content Filtering, this attribute reports the last classification used by system for the flow, or blank if classification was never successfully performed. For URL Blacklisting, specifies category of the blacklisted URL in the Blacklist database.
sn-cf-category-flow-action	For Category-based Content Filtering, this attribute reports the last action taken for the flow, or blank if content filtering was never performed. The following are the possible values: • allow • content-insert • discard • redirect-url • terminate-flow For URL Blacklisting, this attribute reports the last action taken for the flow, or blank if Blacklist matching was never performed. The following are the possible values: • discard • terminate-flow • redirect-url • www-reply-code-terminate-flow
sn-cf-category-policy	For Category-based Content Filtering, this attribute reports the category policy identifier that was used for the flow, or blank if content filtering was never attempted for the flow.
sn-cf-category-rating-type	For Category-based Content Filtering, this attribute reports the type, either “static” or “dynamic” that was last successfully performed for the flow, or blank if content filtering was never successful for the flow. For URL Blacklisting, specifies “blacklisting”.
sn-cf-category-unknown-url	This attribute reports the identifier for unknown URL under content filtering action. It holds either “1” for unknown URLs or “0” for the URLs having static rating in its database.
sn-charge-volume	This attribute reports the total charge volume excluding bytes/packets dropped/retransmitted by ECS. This behavior can be changed by configuring to allow dropped/retransmitted bytes/packets to be included in the net volume. See the **edr sn-charge-volume** command in the *ACS Rulebase Configuration Mode Commands* chapter.

Attributes	Description
sn-closure-reason	This attribute reports the reason for termination of the flow/EDR: • 0: Normal end of flow • 1: End of flow by handoff processing • 2: Subscriber session terminated • 3: Inter-chassis Session Recovery switchover • 12: Completion of transaction
sn-correlation-id	This attribute reports the RADIUS correlation identifier.
sn-direction	This attribute reports the direction of the first packet for the flow. It has following values: • **toMobile**: This value appears when direction of first packet is towards mobile node. • **fromMobile**: This value appears when direction of first packet is towards mobile node. • **unknown**: This value appears when the original originator of a flow can not be determined (for example, a flow that is interrupted due to a Inter-chassis Session Recovery switchover).
sn-duration	This attribute reports the duration between the last and first packet for the record.
sn-end-time [format *format* **] localtime**	This attribute reports the timestamp for last packet of flow in UTC.
sn-fa-correlation-id	This attribute reports the RADIUS Correlation Identifier of the Foreign Agent (FA).
sn-fa-ip-address	This attribute reports IP address of the Foreign Agent (FA).
sn-filler-blank	This attribute inserts a blank filler field, generates an empty EDR field.
sn-filler-zero	This attribute inserts a “0” in the EDR field.
sn-flow-end-time	This attribute reports the time of flow-end EDR generation—when EDRs are generated at hagr, session-end, timeout, or normal-end-signaling conditions. **sn-start-time** and **sn-end-time** fields of flow end-condition EDRs cannot be used to determine the duration of the flow if intermediate EDRs are generated (rule-match or transaction-complete or any other intermediate EDR). **sn-start-time** field in an EDR gives the time the first packet was received after the last EDR was generated. So, whenever an EDR is generated, this field is reset to the time the EDR gets generated. So the **sn-start-time** field in flow end-condition EDRs may not have the time of the first packet received on that flow. It will have the time at which the last EDR was generated or the first packet time if no EDR was generated for that flow. **sn-end-time** field gives the time at which the last packet on the flow was received. Flow end-condition EDRs may not be generated immediately after receiving the last packet. For example, in case of session-end or timeout EDRs, last packet time and EDR generation time may be different. **sn-flow-start-time** gives the time of the first packet of the flow (irrespective of whether intermediate EDRs were generated), and **sn-flow-end-time** gives the time when EDRs are generated at hagr, session-end, timeout or normal-end-signaling conditions. The values of these fields will be populated in EDRs only for hagr, session-end, timeout and normal-end-signaling EDRs.
sn-flow-id	This attribute reports the flow-id assigned internally by the ECS module to each flow.

Attributes	Description
sn-flow-start-time	This attribute reports the time of the first packet of the flow (irrespective of whether intermediate EDRs were generated). Also see, **sn-flow-end-time**.
sn-format-name	This attribute reports the name of the EDR/UDR format used.
sn-group-id	This attribute reports the sequence group ID of the record.
sn-ha-ip-address	This attribute reports IP address of the Home Agent (HA).
sn-nat-binding-timer	For Network Address Translation (NAT) in-line service, this attribute reports the port chunk hold timer.
sn-nat-gmt-offset	For NAT in-line service, this attribute reports the GMT offset of the node generating NAT bind record.
sn-nat-ip	For NAT in-line service, this attribute reports the NAT IP address of the port chunk.
sn-nat-last-activity-time-gmt	For NAT in-line service, this attribute reports the time when the last flow in a specific NAT set of flows was seen.
sn-nat-port-block-end	For NAT in-line service, this attribute reports the last port number of the port chunk.
sn-nat-port-block-start	For NAT in-line service, this attribute reports the starting port number of the port chunk.
sn-nat-port-chunk-alloc-dealloc-flag	For NAT in-line service, this attribute reports whether the port chunk is allocated or released.
sn-nat-port-chunk-alloc-time-gmt	For NAT in-line service, this attribute reports when the port chunk was allocated.
sn-nat-port-chunk-dealloc-time-gmt	For NAT in-line service, this attribute reports when the port chunk was released.
sn-nat-realm-name	For NAT in-line service, this attribute reports the name of the NAT realm.
sn-nat-subscribers-per-ip-address	For NAT in-line service, this attribute reports the subscriber(s) per NAT IP address.
sn-parent-protocol	This attribute reports the parent protocol of the flow. An integer value like in **sn-app-protocol**; for RTCP/RTP flows, the parent protocol may be RTSP or SIP; for GRE flows, the parent protocol will be PPTP, and so on.
sn-rulebase	This attribute reports the name of the ECS rulebase applied.
sn-sequence-no	This attribute reports the unique sequence number (per **sn-sequence-group** and **radius-nas-ip-address**) of EDR identifier and linearly increasing in EDR file.
sn-server-port	This attribute reports the TCP/UDP port number of the server in a subscriber's data flow.
sn-start-time [format *format* **] localtime**	This attribute reports the timestamp for last packet of flow in UTC.
sn-subscriber-nat-flow-ip	For NAT in-line service, this attribute reports the NAT IP address of NAT-enabled subscriber.
sn-subscriber-nat-flow-port	For NAT in-line service, this attribute reports the NAT port number of NAT-enabled subscriber.

Attributes	Description
sn-subscriber-port	This attribute reports the TCP/UDP port number of the Mobile handling subscriber data flow.
sn-volume-amt { ip | tcp } { bytes | pkts } { uplink | downlink }	This attribute reports IP/TCP protocol-specific volume amount of downlink/uplink bytes/packets during a flow. This includes all the bytes/packets received by ECS, including the bytes/packets dropped and retransmitted by ECS.
sn-volume-dropped-amt { ip | tcp } { bytes | packets } { downlink | uplink }	For Stateful Firewall in-line service, this attribute reports IP/TCP protocol-specific volume amount of downlink/uplink bytes/packets dropped by Stateful Firewall during a flow.
sn-volume-ip-with-rtsp-or-rtp bytes { downlink | priority | uplink }	This attribute reports the IP volume amount of downlink/uplink bytes of an RTSP flow and the RTP flows controlled by it, or Comma Separated Value (CSV) position priority of this field. If **uplink** or **downlink** is not specified it shows the total of both.
transaction-downlink-bytes	This attribute reports the total downlink bytes for the transaction.
transaction-downlink-packets	This attribute reports the total downlink packets for the transaction.
transaction-uplink-bytes	This attribute reports the total uplink bytes for the transaction.
transaction-uplink-packets	This attribute reports the total uplink packets for the transaction.

format { MM/DD/YY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds }

Specifies the timestamp format.

localtime

Specifies timestamps with the local time. By default, timestamps are displayed in GMT/UTC.

{ ip | tcp } { bytes | pkts } { downlink | uplink }

Specifies bytes/packets sent/received from/by mobile.

priority *priority*

Specifies the position priority of the value within the EDR record. Lower numbered priorities (across all attribute, event-label, and rule-variable) occur first.
priority must be an integer from 1 through 65535. Up to 50 position priorities (across all attribute, event-label, and rule-variable) can be configured.

Usage

Use this command to set the attributes and priority for EDR file format.
A particular field in EDR format can be entered multiple times at different priorities. While removing the EDR field using the **no attribute** command either you can remove all occurrences of a particular field by specifying the field name or a single occurrence by additionally specifying the optional **priority** keyword.

Example

The following is an example of this command:

```
attribute radius-user-name priority 12
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

event-label

This command allows you to specify an optional event label/identifier to be used as an attribute in the EDRs.

Product

All

Privilege

Security Administrator, Administrator

Syntax

event-label *event_label* **priority** *priority*

no event-label

no

If previously configured, removes the event label configuration.

event_label

Specifies the event label/identifier to be used as EDR attribute.
event_label must be an alphanumeric string of 1 through 63 characters.

priority *priority*

Specifies the Comma Separated Value (CSV) position of the attribute (label/identifier) in the EDR.
priority must be an integer from 1 through 65535.

Usage

Use this command to configure an optional event label/identifier as an attribute in the EDR and its position in the EDR.

Example

The following is an example of this command:

```
event-label radius_csv1 priority 23
```

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

rule-variable

This command allows you to specify fields and their order in EDRs.

Product

All

Privilege

Security Administrator, Administrator

Syntax

rule-variable *rule_variable* **priority** *priority* **[in-quotes]**

no rule-variable *rule_variable* **[priority** *priority* **]**

---

no

If previously configured, removes the specified rule variable configuration.

---

rule_variable

Specifies the rule variable for the EDR format.
rule_variable must be one of the following options:

- **bearer 3gpp**: 3GPP bearer-related fields:
  - **charging-id**: Charging ID of the bearer flow
  - **imei**: IMEI or IMEISV (depending on the case) associated with the bearer flow. Only available in StarOS 8.1 and later releases.
  - **imsi**: Specific Mobile Station Identification number.
  - **rat-type**: RAT type associated with the bearer flow. Only available in StarOS 8.1 and later releases.
  - **sgsn-address**: SGSN associated with the bearer flow. Only available in StarOS 8.1 and later releases. For MIPv6 calls, sgsn-address field is populated with HSGW address.
  - **user-location-information**: User location information associated with the bearer flow. Only available in StarOS 8.1 and later releases.
- **bearer 3gpp2**: 3GPP2 bearer-related fields:
  - **always-on**: 3GPP2 always on indicator
  - **bsid**: 3GPP2 BSID
  - **esn**: 3GPP2 ESN
  - **ip-qos**: 3GPP2 IP QoS
  - **ip-technology**: 3GPP2 IP technology
  - **release-indicator**: 3GPP2 release indicator
  - **service-option**: 3GPP2 service option
  - **session-begin**: 3GPP2 session begin indicator
  - **session-continue**: 3GPP2 session continue indicator

- **bearer ggsn-address**: GGSN IP address field. For MIPv6 calls, ggsn-address field in EDR will be populated with PGW address.
- **dns**: Domain Name System (DNS) related fields:
  - **answer-name**: DNS answer name. This depends upon query type.
  - **previous-state**: DNS previous state information
  - **query-name**: DNS query name
  - **return-code**: DNS query response code
  - **state**: DNS current state information
  - **tid**: DNS Transaction Identifier
- **file-transfer**: File Transfer related fields:
  - **chunk-number**: Number of chunks
  - **current-chunk-length**: Length of current chunk
  - **declared-chunk-length**: Declared size of the chunk
  - **declared-file-size**: Declared size of the file
  - **filename**: Name of the file being transferred
  - **previous-state**: Previous state of session
  - **state**: Current state of session
  - **transferred-file-size**: Transferred size of the file
- **flow**:Flow related fields:
  - **tethered**: Tethering detected on flow. Enables/disables tethering detection result field in EDRs sent to MUR.
- **ftp**: File Transfer Protocol (FTP) related fields:
  - **client-ip-address**:
  - **client-port**
  - **command name**: Command sent
  - **connection-type**
  - **filename**: File name being transferred in any of the FTP-related FTP command
  - **pdu-length**: FTP PDU length
  - **pdu-type**
  - **previous-state**: Previous state of FTP session
  - **reply code**
  - **server-ip-address**
  - **server-port**
  - **session-length**: Total length of FTP session
  - **state**: Current state of FTP session
  - **url**: URL of file
  - **user**: User identifier

- **http**: Hypertext Transport Protocol (HTTP) related fields:
  - **ad-delivered**: advertisement delivered using TPO text-with-click
  - **ad-replaced**: advertisement replaced with TPO 0-byte response
  - **attribute-in-data**: dynamic header field in application payload
  - **attribute-in-url**: dynamic header field in URL
  - **compression-bytes-in**: TPO compression bytes in
  - **compression-bytes-out**: TPO compression bytes out
  - **content disposition**
  - **content length**
  - **content type**
  - **domain**
  - **dns-resolution-locally**: TPO DNS resolution done locally
  - **dns-resolution-remotely**: TPO DNS resolution done remotely
  - **header-length**: HTTP header length
  - **host**
  - **payload-length**: Payload length
  - **pdu-length**
  - **previous-state**: Previous state of session
  - **referer**
  - **reply code**: HTTP response
  - **request method**: HTTP request method
  - **session-length**: Total length of HTTP session
  - **state**: Current state of session
  - **tpo-enabled**: TPO enabled/disabled for HTTP
  - **transaction-length**: Total length of HTTP transaction
  - **transfer-encoding**: Transfer encoding
  - **uri**: Uniform Resource Identifier
  - **url**: Uniform Resource Locator
  - **user-agent**
  - **version**
  - **x-header**: extension header
- **icmp**: Internet Control Message Protocol (ICMP) related fields:
  - **code**: ICMP code
  - **type**: ICMP type
- **icmpv6**: Internet Control Message Protocol Version 6 (ICMPv6) related fields:
  - **code**: ICMPv6 code
  - **type**: ICMPv6 type

- **imap**: Internet Message Access Protocol (IMAP) related fields:
  - **cc**: IMAP e-mail CC field
  - **command**: IMAP command
  - **content**
  - **date**: IMAP e-mail Date field
  - **final-reply**: IMAP final reply
  - **from**: IMAP e-mail From field
  - **mail-size**: IMAP size of e-mail in RFC822 format
  - **mailbox-size**: IMAP number of e-mails in the mailbox
  - **message-type**: IMAP message type
  - **previous-state**: IMAP session previous state
  - **session-length**: IMAP session length
  - **session-previous-state**: IMAP session previous state
  - **session-state**: IMAP session state
  - **state**: IMAP state
  - **subject**: IMAP e-mail Subject field
  - **to**: IMAP e-mail To field
- **ip**: Internet Protocol (IP) related fields:
  - **dst-address**: destination IP address
  - **protocol**: Protocol being transported by IP packet
  - **server-ip-address**: IP address of server. This field in EDR contains either the IPv4 or IPv6 address of the server for a particular flow (flow level). The maximum length of this field is 48 characters. For an IPv6 address, the maximum length is 45 characters; for an IPv4 address, the maximum length is 15 characters.
  - **src-address**: Source IP address
  - **subscriber-ip-address**: IP address of subscriber. This field in EDR contains either the IPv4 or IPv6 address of the client/subscriber for a particular call (subscriber level). The value of this field does not change for a particular call. The maximum length of this field is 48 characters. For an IPv6 address, the maximum length is 45 characters. For an IPv4 address, the maximum length is 15 characters.
  - **total-length**: Total length of packet, including payload
  - **version**: IP version
- **mms**: Multimedia Message Service (MMS) related fields:
  - **bcc**
  - **cc**
  - **content location**
  - **content type**
  - **date [format { MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS }]**
  - **from**

- **message-size**
- **previous-state**
- **response status**
- **state**
- **subject**
- **tid**
- **to**

- **p2p protocol:** Peer-to-peer protocol field.
- **pop3**: Post Office Protocol version 3 (POP3) related fields:
  - **command name**: Command of POP3 session
  - **mail-size**: Mail size
  - **pdu-length**: Length of POP3 PDU
  - **pdu-type**: Type of packet
  - **previous-state**: Previous state of POP3 session
  - **reply status**: Reply for the POP3 command
  - **session-length**: Total length of POP3 session
  - **state**: Current state of POP3 session
  - **user-name**: User of POP3 session
- **rtcp:** RTP Control Protocol (RTCP) related fields:
  - **control-session-flow-id**: Flow ID of the controlling RTSP/SIP session
  - **jitter**: RTCP interarrival jitter
  - **rtsp-id**: RTSP ID of the RTCP flow
  - **uri**: URI of the control protocol related to the RTCP flow
- **rtp**: Real-time Transfer Protocol (RTP) related fields:
  - **control-session-flow-id**: Flow ID of the controlling RTSP/SIP session
  - **pdu-length**: Length of RTP PDU
  - **rtsp-id**: RTSP ID of the flow
  - **session-length**: Total length of RTP session
  - **uri**: URI of the control protocol related to the RTP flow
- **rtsp**: Real Time Streaming Protocol (RTSP) related fields:
  - **command-id**: RTSP command ID
  - **content type**
  - **date**: RTSP Date field
  - **previous-state**: RTSP previous state
  - **reply code**
  - **request method 1**: play method
  - **request method 2**: setup method

- **request method 3**: pause method
- **request method 4**: record method
- **request method 5**: options method
- **request method 6**: redirect method
- **request method 7**: describe method
- **request method 8**: announce method
- **request method 9**: teardown method
- **request method 10**: get-parameter method
- **request method 11**: set-parameter method
- **request packet**
- **rtp-uri**: RTSP RTP-Info stream-uri field
- **session-id**: RTSP session-id field
- **session-length**: Total number of bytes passed through the RTSP data session
- **state**: RTSP state
- **uri**: RTSP uri field
- **uri sub-part**
- **user-agent**: RTSP user-agent field

- **sdp**: Session Description Protocol (SDP) related fields:
  - **connection-ip-address**: IP address in SDP connection field
  - **media-audio-port**: Port used for audio media
  - **media-video-port**: Port used for video media
- **secure-http**: HTTPS related field.
- **sip**: Session Initiation Protocol (SIP) related fields:
  - **call-id**: SIP call-id field
  - **content type**
  - **from**: SIP From field
  - **previous-state**: SIP previous state
  - **reply code**
  - **request method**
  - **request packet**
  - **state**: SIP state
  - **to**: SIP To field
  - **uri**: SIP URI field
  - **uri sub-part**
- **smtp**: Simple Mail Transfer Protocol (SMTP) related fields:
  - **command name**: Command of SMTP session
  - **mail-size**: Size of given mail

- **pdu-length**: Length of SMTP PDU
- **previous-state**: Previous state of SMTP session
- **recipient**: SMTP e-mail Recipient field
- **reply status**: Response for the SMTP command
- **sender**: SMTP e-mail Sender field
- **session-length**: Total length of SMTP session
- **state**: Current state of SMTP session

- **tcp**: Transmission Control Protocol (TCP) related fields:
  - **dst-port**: TCP destination port
  - **duplicate**: TCP retransmitted/duplicate packet
  - **flag**: Current packet TCP flag
  - **os-signature**: OS signature string for TCP flow. Enables/disables OS Signature field in EDRs sent to MUR.
  - **out-of-order**: TCP out of order packet analyzed
  - **payload-length**: TCP payload length
  - **previous-state**: Previous state of MS
  - **src-port**: TCP source port
  - **state**: Current state of MS
  - **tpo-enabled**: TPO enabled/disabled for TCP
- **traffic-type**: Traffic type of flow (voice or non-voice depending upon flow type).
- **udp**: User Datagram Protocol (UDP) related fields:
  - **dst-port**: UDP destination port
  - **src-port**: UDP source port
- **voip-duration**: Duration of voice call, in seconds. For a flow in which voice call end is detected, output will be a non-zero value. For other flows it will be zero.
- **wsp**: Wireless Session Protocol (WSP) related fields:
  - **content type**
  - **domain**: WSP domain name
  - **host**: WSP host name
  - **pdu-length**: WSP PDU length
  - **pdu-type**: WSP PDU type
  - **reply code**
  - **session-length**: WSP total packet length
  - **tid**: WSP transaction identifier
  - **total-length**: WSP total packet length
  - **url**: WSP URL
  - **user-agent**: WSP user agent

- **wtp**: Wireless Transaction Protocol (WTP) related fields:
  - **gtr**: Group Transmission Flag
  - **pdu-length**: PDU length of the WTP packet
  - **pdu-type**: WTP protocol data unit information
  - **previous-state**: WTP previous state information
  - **state**: WTP current state information
  - **tid**: WTP transaction identifier
  - **transaction class**: WTP transaction class
  - **ttr**: WTP Trailer Transmission flag

Important: For more information on protocol-based rules, see the *ACS Ruledef Configuration Mode Commands* chapter.

priority *priority*

Specifies the CSV position of the field (protocol rule) in the EDR.
priority must be an integer from 1 through 65535.

in-quotes

Specifies placing double quotes (“ ”) around the specified field in the EDR.

Important: In this release, this keyword is only valid for the MMS protocol **to** and **subject** fields. **rule-variable mms to priority** *priority* **[in-quotes] rule-variable mms subject priority** *priority* **[in-quotes]**

Usage

Use this command to specify what field appears in which order in the EDR.
A particular field in an EDR format can be entered multiple times with different priorities. While removing the EDR field using the **no rule-variable** command you can remove all occurrences of a particular field by specifying the field name or a single occurrence by additionally specifying the optional **priority** keyword.

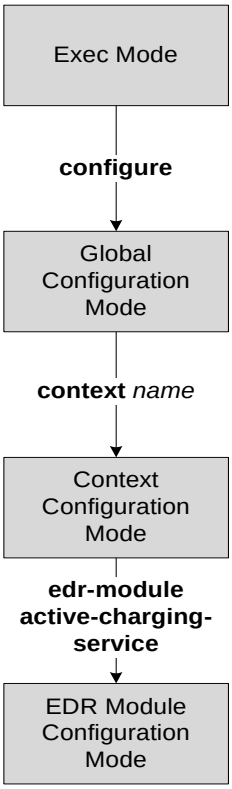
Example

The following is an example of this command:

```
rule-variable tcp dst-port priority 36
```

Chapter 107
EDR Module Configuration Mode Commands

The EDR Module Configuration Mode allows you to configure Event Data Record (EDR) file transfer parameters.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

cdr

This command allows you to configure EDR/UDR file transfer parameters.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
cdr { purge { storage-limit storage_limit | time-limit time_limit } [ max-files
max_records_to_purge ] | push-interval push_interval | push-trigger space-usage-percent
trigger_percentage | remove-file-after-transfer | transfer-mode { pull [ module-only ] |
push primary { encrypted-url encrypted_url | url url } [ [ max-files max_records ] [
module-only ] [ secondary { encrypted-secondary-url encrypted_secondary_url | secondary-
url secondary_url } ] [ via local-context ] + ] | use-harddisk }

default cdr [ purge | push-interval | push-trigger space-usage-percent | remove-file-
after-transfer | transfer-mode [ module-only | push via ] | use-harddisk ] +

no cdr [ purge | remove-file-after-transfer | use-harddisk ] +
```

default

Configures the default setting for the specified keyword(s):

- **purge**: Disabled
- **push-interval**: 300 seconds
- **push-trigger**: 80 percent
- **remove-file-after-transfer**: Disabled
- **transfer mode**: Pull
- **push via**: LC is used for push
- **use-harddisk**: Disabled

Important: The **use-harddisk** keyword is available only on the ASR 5000 chassis.

no

If previously configured, disables the specified configuration:

- **purge**: Disables purging of records.
- **remove-file-after-transfer**: Retains a copy of the file even after it has been pushed or pulled to another server.
- **use-harddisk**: Disables data storage on the SMC hard disk.

Important: The **use-harddisk** keyword is available only on the ASR 5000 chassis.

purge { storage-limit *storage_limit* **| time-limit** *time_limit* **} [max-files** *max_records_to_purge* **]**

Specifies to purge/delete the CDR/EDR records based on "time" or "volume" limit.

- **storage-limit** *storage_limit*: Specifies to start deleting files when the specified megabytes of space is used for storage. *storage_limit* specifies the volume limit for the record files, in megabytes, and must be an integer from 10 through 143360.
- **time-limit** *time_limit*: Specifies to start deleting files older than the specified time limit. *time_limit* specifies the time limit for the record files, and must be an integer from 600 through 2592000.
- **max-files** *max_records_to_purge*: Specifies the maximum number of records to purge. *max_records_to_purge* must be an integer from 1000 through 10000.

push-interval *push_interval*

Specifies the transfer interval (in seconds) to push EDR and UDR files to an external file server. *push_interval* must be an integer from 60 through 3600.
Default: 300

push-trigger space-usage-percent *trigger_percentage*

Specifies the EDR/UDR disk space utilization percentage, upon reaching which an automatic push is triggered and files are transferred to the configured external server.
trigger_percentage specifies the EDR/UDR disk utilization percentage for triggering push, and must be an integer from 10 through 80.
Default: 80

remove-file-after-transfer

Specifies that the system must delete EDR/UDR files after they are transferred to the external file server.
Default: Disabled

transfer-mode { pull [module-only] | push primary { encrypted-url *encrypted_url* **| url** *url* **} [[max-files** *max_records* **] [module-only] [secondary { encrypted-secondary-url** *encrypted_secondary_url* **| secondary-url** *secondary_url* **}] [via local-context] +]**

Specifies the EDR/UDR file transfer mode—how the EDR and UDR files are transferred to an external file server.

- **pull**: Specifies that the L-ESS is to pull the CDR files.
- **push**: Specifies that the system is to push CDR files to the configured L-ESS.
- **max-files** *max_records*: Specifies the maximum number of files sent per iteration based on configured file size.

  Default: 4000
- **module-only**: Specifies that the transfer-mode is only applicable to the EDR module; if not configured it is applicable to both EDR and UDR modules. This enables to support individual record transfer-mode configuration for each module.
- **primary encrypted-url** *encrypted_url*: Specifies the primary URL location in encrypted format to which the system pushes the CDR files.

  encrypted_url must be the location in an encrypted format, and must be an alphanumeric string of 1 through 1024 characters.

- **primary url** *url*: Specifies the primary URL location to which the system pushes the CDR files.

  url must be the location, and must be an alphanumeric string of 1 through 1024 characters in the "*//user:password@host:[port]/directory*" format.

- **secondary encrypted-secondary-url** *encrypted_secondary_url*: Specifies the secondary URL location in encrypted format to which the system pushes the CDR files when the primary location is unreachable or fails.

  encrypted_secondary_url must be the secondary location in an encrypted format, and must be an alphanumeric string of 1 through 1024 characters in the "*//user:password@host:[port]/directory*" format.

- **secondary secondary-url** *secondary_url*: Specifies the secondary location to which the system pushes the CDR files when the primary location is unreachable or fails.

  secondary_url must be the secondary location, and must be an alphanumeric string of 1 through 1024 characters in the "*//user:password@host:[port]/directory*" format.

- **via local-context**: Configuration to select LC/SPIO for transfer of CDRs. The system pushes the EDR files via SPIO in the local context.

use-harddisk

Important: The **use-harddisk** keyword is available only on the ASR 5000 chassis.

Specifies that on the ASR 5000 chassis the hard disk on the SMC be used to store EDR/UDR files. On configuring to use the hard disk for EDR/UDR storage, EDR/UDR files are transferred from packet processing cards to the hard disk on the SMC. Default: Disabled

+

Indicates that more than one of the previous keywords can be entered within a single command.

Usage

Use this command to configure how the charging data records (CDR) are moved and stored.
On the ASR 5000 chassis, you must run this command only from the local context. If you run this command in any other context it will fail and result in an error message.
If PUSH transfer mode is configured, the L-ESS server URL to which the CDR files need to be transferred to must be specified. The configuration allows a primary and a secondary server to be configured. Configuring the secondary server is optional. Whenever a file transfer to the primary server fails for four consecutive times, the files will be transferred to the secondary server. The transfer will switch back to the original primary server when:

- Four consecutive transfer failures to the secondary server occur.
- After switching from the primary server, 30 minutes elapses.

When changing the transfer-mode from pull to push, disable the PULL from L-ESS and then change the transfer mode to push. Make sure that the push server URL configured is accessible from the local context. Also, make sure that the base directory that is mentioned contains udr directory created within it.
When changing the transfer mode from push to pull, after changing, enable PULL on the L-ESS. Any of the ongoing PUSH activity will continue till all the scheduled file transfers are completed. If there is no PUSH activity going on at the time of this configuration change, all the PUSH related configuration is nullified immediately.

The **cdr use-harddisk** command is available only on the ASR 5000 chassis. This command can be run only in a context where CDRMOD is running. Configuring in any other context will result in failure with the message *"Failure: Please Check if CDRMOD is running in this context or not."*
The **cdr use-harddisk** command can be configured either in the EDR or UDR module, but will be applicable to both record types. Configuring in one of the modules will prevent the configuration to be applied in the other module. Any change to this configuration must be done in the module in which it was configured, the change will be applied to both record types.
The VPNMgr can send a maximum of 4000 files to the remote server per iteration. However if the individual file size is big (say when compression is not enabled), then while transferring 4000 files SFTP operation takes a lot of time. To prevent this, the **cdr transfer-mode push** command can be configured with the keyword **max-files**, which allows operators to configure the maximum number of files sent per iteration based on configured file size.

Example

The following command retains a copy of the data file after it has been transferred to the storage location:

```
no cdr remove-file-after-transfer
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

file

This command allows you to configure EDR file parameters.

Product

All

Privilege

Security Administrator, Administrator

Syntax

file [charging-service-name { include | omit }] [compression { gzip | none }] [current-prefix *string* **] [delete-timeout** *seconds* **] [directory** *directory_name* **] [edr-format-name] [exclude-checksum-record] [field-separator { hyphen | omit | underscore }] [file-sequence-number rulebase-seq-num] [headers] [name** *file_name* **] [reset-indicator] [rotation [num-records** *number* **| time** *seconds* **| volume** *bytes* **]] [sequence-number { length** *length* **| omit | padded | padded-six-length | unpadded }] [storage-limit** *limit* **] [single-edr-format] [time-stamp { expanded-format | rotated-format | unix-format }] [trailing-text** *string* **] [trap-on-file-delete] [xor-final-record] +**

default file [charging-service-name] [compression] [current-prefix] [delete-timeout] [directory] [edr-format-name] [field-separator] [file-sequence-number] [headers] [name] [reset-indicator] [rotation { num-records | time | volume }] [sequence-number] [storage-limit] [time-stamp] [trailing-text] +

---

default

Configures the default setting for the specified keyword(s).

---

charging-service-name { include | omit }

Specifies to include/exclude name of the charging service in the file name.

- **include**: Include name of the charging service in the EDR file name.
- **omit**: Exclude name of the charging service in EDR file name.

---

compression { gzip | none }

Specifies compression of EDR files.

- **gzip**: Enables GNU zip compression of the EDR file at approximately 10:1 ratio.
- **none**: Disables Gzip compression.

---

current-prefix *string*

Specifies a string to add to the beginning of the EDR file that is currently being used to store EDR records.
string must be an alphanumeric string of 1 through 31 characters.
Default: **curr**

---

delete-timeout *seconds*

Specifies a timeout period (in seconds) when completed EDR files are deleted. By default, files are never deleted.
seconds must be an integer from 3600 through 31536000.

Default: Disabled

directory *directory_name*

Specifies a subdirectory in the default directory in which to store EDR files.
directory_name must be an alphanumeric string of 1 through 191 characters.
Default: **/records/edr**

edr-format-name

Specifies creation of separate files for EDRs that have different formats. Name of the EDR format is included in the file name.

exclude-checksum-record

When entered, this keyword excludes the final record containing #CHECKSUM followed by the 32-bit Cyclic redundancy check (CRC) of all preceding records from the EDR file.
Default: Disabled (inserts checksum record into the EDR file header)

field-separator [hyphen | omit | underscore]

Specifies the field inclusion/exclusion type of separators between two fields of EDR file name:

- **hyphen**: Specifies to use "-" (hyphen) as the field separator.
- **omit**: Excludes the field separator.
- **underscore**: Specifies to use "_" (underscore) as the field separator.

file-sequence-number rulebase-seq-num

Specifies that the file name sequence numbers must be unique per rulebase and EDR format name combination.

headers

Includes a file header summarizing the record layout.

name *file_name*

Specifies a string to be used as the base file name for EDR files.
Default: **edr**
file_name must be an alphanumeric string of 1 through 31 characters. The file name format is as follows:
base_rulebase_format_sequencenum_timestamp

- *base*: Specifies the type of record in file or contains the operator-specified string.

  Default: edr

- *rulebase*: Specifies the name of the ACS rulebase. EDRs from different rulebases go into different EDR files.
- *format*: Specifies the name of the EDR format if **single-edr-format** is specified, else the format field (and the trailing underscore) is omitted from the file name.
- *sequencenum*: This is a 5-digit sequence number to detect the missing file sequence. It is unique among all EDR files on the system.
- *timestamp*: Contains a timestamp based on file creation time in UTC time in MMDDYYYYHHMMSS format.

EDR files that have not been closed have a string added to the beginning of their filenames.

Filename for an EDR file in CSV format that contains information for rulebase named *rulebase1* and an EDR schema named *edr_schema1* appears as follows:
edr_rulebase1_edr_schema1_00005_01302006143409
If the file name is not configured the system will create files for EDRs/UDRs/FDRs (xDRs) using the following template with limits to 256 characters:
basename_ChargSvcName_timestamp_SeqNumResetIndicator_FileSeqNumber

- *basename*: A global-based configurable text string that is unique per system that uniquely identifies the global location of the system running ACS.
- *ChargSvcName*: A system context-based configurable text string that uniquely identifies a specific context-based charging service
- *timestamp*: Date and time at the instance of file creation. Date and time in the form of "MMDDYYYYHHmmSS" where HH is a 24-hour value from 00-23
- *SeqNumResetIndicator*: A one-byte counter used to discern the potential for duplicated FileSeqNumber with a range of 0 to 255, which is incremented by a value of 1 for the following conditions:
  - Failure of an ACS software process on an individual PSC.
  - Failure of the system such that a second system takes over. For example, a backup or standby system put in place according to Interchassis Session Recovery.
  - File Sequence Number (FileSeqNumber) rollover from 999999999 to 0
- *FileSeqNumber*: Unique file sequence number for the file with 9 digit integer having range from 000000000 to 999999999. It is unique on each system.

File name for a closed xDR file in CSV format that contains information for ACS system *xyz_city1* and charging service name *preapaid2* with timestamp *12311969190000*, and file sequence number counter reset indicator to *002* for file sequence number *034939002* appears as follows:
xyz_city1_preapaid2_12311969190000_002_034939002
File name for a running xDR file, not closed, in CSV format that contains information for the same parameters for file sequence number *034939003* prefixed with *curr_* and appears as follows:
curr_xyz_city1_preapaid2_12311969190000_002_034939002

---

reset-indicator

Specifies inclusion of the reset indicator counter value, from 0 through 255, in the EDR file name, and is incremented (by one) whenever any of the following conditions occur:

- An ACSMgr/SessMgr process fails.
- A peer chassis has taken over in compliance with our Interchassis Session Recovery feature.
- The sequence number, see the **sequence-number** keyword, has rolled over to zero.

---

rotation { num-records *number* **| time** *seconds* **| volume** *bytes* **}**

Specifies when to close an EDR file and create a new one.

- **num-records** *number*: Specifies the number of records that should be added to the file. When the number of records in the file reaches the specified value, the file is complete.

  number must be an integer from 100 through 10240.

  Default: 1024

- **time** *seconds*: Specifies the period of time (in seconds) to wait before closing the EDR file and creating a new one.

  seconds must be an integer from 30 through 86400.

Default: 3600

- **volume** *bytes*: Specifies the maximum size (in bytes) of the EDR file before closing it and creating a new one.

  bytes must be an integer from 51200 through 62914560.

  Note that a higher setting may improve the compression ratio when the compression keyword is set to gzip.

---

sequence-number { length *length* **| omit | padded | padded-six-length | unpadded }**

Specifies including/excluding sequence number in the file name.

- **length** *length*: Includes the sequence number with the specified length.

  length must be the length of the file sequence number, with preceding zeroes, in the file name, and must be an integer from 1 through 9.

  > ***Important:*** The **length** keyword is applicable in both EDR and UDR modules. When applied in both modules without the **file udr-seq-num** configuration, the minimum among the two values will come into effect for both the modules. With the **file udr-seq-num** keyword, each module will use its own value of length.

- **omit**: Excludes the sequence number from the file name.
- **padded**: Includes the padded sequence number with preceding zeros in the file name. This is the default setting.
- **padded-six-length**: Includes the padded sequence number with six preceding zeros in the file name.
- **unpadded**: Includes the unpadded sequence number in the file name.

---

single-edr-format

Creates separate files for EDRs having different formats.
Default: Disabled

---

storage-limit *limit*

Specifies deleting files when the specified amount of space (in bytes) is used up for EDR/UDR file storage RAM on packet processing cards.
limit must be an integer from 10485760 through 536870912. Default: 33554432

---

time-stamp { expanded-format | rotated-format | unix-format }

Specifies the timestamp of when the file was created be included in the file name.

- **expanded-format**: Specifies the UTC MMDDYYYYHHMMSS format.
- **rotated-format**: Specifies the time stamp format to YYYYMMDDHHMMSS format.
- **unix-format**: Specifies the UNIX format of *x.y*, where *x* is the number of seconds since 1/1/1970 and *y* is the fractional portion of the current second that has elapsed.

---

trailing-text *string*

Specifies the inclusion of an arbitrary text string in the file name.
string must be an alphanumeric string of 1 through 30 characters.

trap-on-file-delete

Instructs the system to send an SNMP notification (trap) when an EDR/UDR file is deleted due to lack of space.
Default: Disabled

xor-final-record

Specifies inserting an XOR checksum (in place of the CRC checksum) into the EDR file header if the **exclude-checksum-record** is left at its default setting.
Default: Disabled

+

Indicates that more than one of the keywords can be entered in a single command.

Usage

Use this command to configure EDR file characteristics.

Example

The following command sets the prefix of the current active EDR file to *Current*:

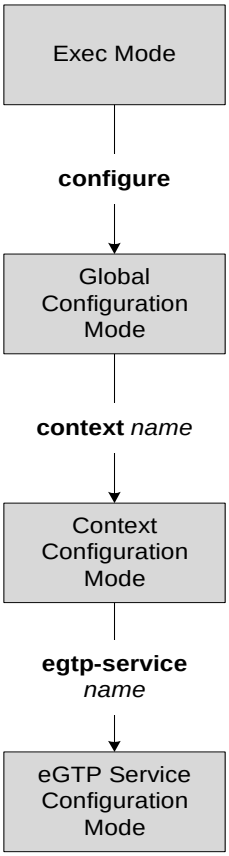
```
file current-prefix Current
```

The following command sets the base file name to *EDRfile*:

```
file name EDRfile
```

Chapter 108
eGTP Service Configuration Mode Commands

The eGTP Service Configuration Mode is used to create and manage Evolved GPRS Tunneling Protocol (eGTP) interface types and associated parameters.



associate

Configures an association with a GTP-U service where parameters are applied to the GTP-U data flow.

Product

P-GW

Privilege

Administrator

Syntax

associate gtpu-service *name*

no associate gtpu-service

no

Removes the association to the configured GTP-U service from this service.

gtpu-service *name*

Associates a GTP-U service with this eGTP service. *name* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to associate a GTP-U service with this eGTP service.

Example

The following command associates this eGTP service with a GTP-U service named *gtpu3*:

```
associate gtpu-service gtpu3
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

gtpc

Configure the GPRS Tunneling Protocol Control (GTP-C) plane settings for this service.

Product

MME, P-GW, S-GW

Privilege

Administrator

Syntax

gtpc { bind { ipv4-address *ipv4_address* **[ipv6-address** *ipv6_address* **] | ipv6-address** *ipv6_address* **[ipv4-address** *ipv4_address* **] } | echo-interval** *seconds* **| ip qos-dscp {** *forwarding_type* **} | max-retransmissions** *num* **| path-failure detection-policy echo | retransmission-timeout** *seconds* **}**

no gtpc { bind { ipv4-address *ipv4_address* **[ipv6-address** *ipv6_address* **] | ipv6-address** *ipv6_address* **[ipv4-address** *ipv4_address* **] } | echo-interval | path-failure detection-policy }**

default gtpc { echo-interval | ip qos-dscp | max-retransmissions | path-failure detection-policy | retransmission-timeout }

---

no

Disables or removes the configured GTP-C setting.

---

default

Resets the specified parameter to its default value.

---

bind { ipv4-address *ipv4_address* **[ipv6-address** *ipv6_address* **] | ipv6-address** *ipv6_address* **[ipv4-address** *iv4p_address* **] }**

Binds the service to an interface with an IPv4 address, IPv6 address or both.
ipv4-address *ipv4_address* **[ipv6-address** *ipv6_address* **]**: Binds this service to the IPv4 address of a configured interface. Optionally, bind the service to a configured interface with an IPv6 address. *ipv4_address* must be entered using IPv4 dotted-decimal notation. *ipv6_address* must be entered using IPv6 colon-separated notation.
ipv6-address *ipv6_address* **[ipv4-address** *ipv4_address* **]**: Binds this service to the IPv6 address of a configured interface. Optionally, bind the service to a configured interface with an IPv4 address. *ip6_address* must be entered using IPv6 colon-separated notation. *ipv4_address* must be entered using IPv4 dotted-decimal notation.

---

echo-interval *seconds*

Configures the duration (in seconds) between the sending of echo messages as an integer from 60 through 3600. Default: 60

ip qos-dscp { *forwarding_type* **}**

Specifies the IP QoS DSCP per-hop behavior to be marked on the outer header of signalling packets originating from the LTE component. This is a standards-based feature (RFC 2597). The following forwarding types are supported:
af11: Designates the use of Assured Forwarding 11 per-hop behavior. This is the default setting.
af12: Designates the use of Assured Forwarding 12 per-hop behavior.
af13: Designates the use of Assured Forwarding 13 per-hop behavior.
af21: Designates the use of Assured Forwarding 21 per-hop behavior.
af22: Designates the use of Assured Forwarding 22 per-hop behavior.
af23: Designates the use of Assured Forwarding 23 per-hop behavior.
af31: Designates the use of Assured Forwarding 31 per-hop behavior.
af32: Designates the use of Assured Forwarding 32 per-hop behavior.
af33: Designates the use of Assured Forwarding 33 per-hop behavior.
af41: Designates the use of Assured Forwarding 41 per-hop behavior.
af42: Designates the use of Assured Forwarding 42 per-hop behavior.
af43: Designates the use of Assured Forwarding 43 per-hop behavior.
be: Designates the use of Best Effort forwarding per-hop behavior.
ef: Designates the use of Expedited Forwarding per-hop behavior typically dedicated to low-loss, low-latency traffic.
The assured forwarding behavior groups are listed in the table below.

	Class 1	Class 2	Class 3	Class 4
Low Drop	AF11	AF21	AF31	AF41
Medium Drop	AF12	AF22	AF32	AF42
High Drop	AF13	AF23	AF33	AF43

Traffic marked with a higher class is given priority during congestion periods. If congestion occurs to traffic with the same class, the packets with the higher AF value are dropped first.

max-retransmissions *num*

Configures the maximum number of retries for packets as an integer from 0 through 15. Default: 4

path-failure detection-policy echo

Enables session cleanup upon path failure detected via ECHO timeout toward a peer. Default: enabled
If disabled, there is no session cleanup upon path failure detected via ECHO timeout toward a peer; however, SNMP trap/logs will continue to indicate path failure.

retransmission-timeout *seconds*

Configures the control packet (echo message) retransmission timeout in GTP (in seconds) as an integer from 1 through 20. Default: 5

Usage

Use this command to configure GTP-C settings for the current service. This interface assumes the characteristics of an S11 reference point on the S-GW or MME.

Example

The following command binds the service to a GTP-C interface with an IP address of *112.334.556.778*:

```
gtpc bind address 112.334.556.778
```

interface-type

Configures the interface type used by this service.

Product

MME, P-GW, S-GW

Privilege

Administrator

Syntax

```
interface-type { interface-mme | interface-pgw-ingress | interface-sgsn | interface-sgw-egress | interface-sgw-ingress }
```

{ interface-mme | interface-pgw-ingress | interface-sgsn | interface-sgw-egress | interface-sgw-ingress }

interface-mme: Specifies that the interface has the characteristics of an eGTP MME S11 reference point to/from an S-GW or an eGTP MME Sv reference point to/from a Mobile Switching Center (MSC).
interface-pgw-ingress: Specifies that the interface has the characteristics of an eGTP P-GW S5/S8 reference point from an S-GW. The interface assumes the characteristics of either a GTP-C (control Plane) or GTP-U (user plane) reference point.
interface-sgsn: Specifies that the interface has the characteristics of an eGTP S-GW S4 reference point to/from an SGSN.
interface-sgw-egress: Specifies that the interface has the characteristics of an eGTP S-GW S5/S8 reference point to an eGTP P-GW. The interface assumes the characteristics of either a GTP-C (control Plane) or GTP-U (user plane) reference point.
interface-sgw-ingress: Specifies that the interface has the characteristics of:

- an eGTP-C S-GW S11 reference point from the MME.
- an eGTP-U S-GW S1-U reference point from the eNodeB.

Usage

Use this command to specify the type of interface this service uses. By configuring this command, the interface takes on the characteristics of the selected type.

Example

The following command configures the interface bound to this service to maintain the characteristics of an eGTP-C S-GW S11 reference point from an MME:

```
interface-type interface-sgw-ingress
```

validation-mode

Configures the type of validation to be performed on messages received by this service.

Product

P-GW

Privilege

Administrator

Syntax

```
validation-mode { custom1 | standard }

default validation-mode
```

default

Returns the command to the default setting of **standard**.

{ custom1 | standard }

custom1: Specifies that the message should be validated based on a vendor-specific set of mandatory elements.
standard: Specifies that the message should be validated based on the set of mandatory elements as defined in 3GPP 29.274.

Usage

Use this command to specify the type of validation performed on messages received by this service. The information elements contained in messages have mandatory elements and conditional elements. The standard set of elements, as defined by 3GPP 29.274 is checked if this command is set to “standard”. The custom1 setting is for a vendor-specific set of mandatory elements.

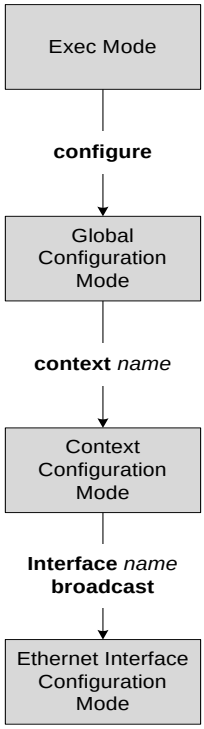
Example

The flowering command sets the validation mode for incoming messages to *standard*:

```
validation-mode standard
```

Chapter 109
Ethernet Interface Configuration Mode Commands

The Ethernet Interface Configuration Mode is used to create and manage the IP interface parameters within a specified context.



crypto-map

Applies the specified IPSec crypto-map to this interface.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

crypto-map *map_name* **[secondary-address** *sec_ip_addr* **]**

no

Deletes the application of the crypto map on this interface.

map_name

Specifies the name of the crypto map being applied as an alphanumeric string of 1 through 127 characters that is case sensitive.

secondary-address *sec_ip_addr*

Applies the crypto map to the secondary address for this interface. *sec_ip_addr* must be specified using the IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

In order for ISAKMP and/or manual crypto maps to work, they must be applied to a specific interface using this command. Dynamic crypto maps should **not** be applied to interfaces.
The crypto map must be configured in the same context as the interface.

Example

To apply the IPSec crypto map named cmap1 to this interface, use the following command:

```
crypto-map cmap1
```

description

Sets the descriptive text for the current interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

description *text*

no description

no

Clears the description for the interface.

text

Specifies the descriptive text as an alphanumeric string of 0 through 79 characters.

Usage

Set the description to provide useful information on the interface's primary function, services, end users, etc. Any information useful may be provided.

Example

```
description sampleInterfaceDescriptiveText
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

ip

Configures the IP options for the current interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip { access-group *acl_name* **{ in | out } [** *priority-value* **] | address** *ip_address ip_mask* **[secondary | srp-activate] | arp { arpa | timeout** *seconds* **} }**

no ip { access-group *acl_name* **{ in | out } | address** *ip_address* **| arp { arpa | timeout } }**

no

Disables and/or restores the option to the system default.

access-group *acl_name* **{ in | out } [** *priority-value* **]**

Specifies the access control list to be added/removed from the group. The ACL rules must be configured in the same context as the interface.
In Release 8.1 and later, *acl_name* must be an alphanumeric string of 1 through 47 characters.
In Release 8.0 and earlier, *acl_name* must be an alphanumeric string of 1 through 79 characters.
The direction must also be specified as either inbound or outbound using the keywords **in** and **out**, respectively.
priority-value: Default: 0. If more than one ACL is applied, *priority-value* specifies the priority in which they will be compared against the packet. If not specified, the priority is set to 0. *priority-value* must be an integer from 0 through 4294967295. If access groups in the list have the same priority, the last one entered is used first.

Important: Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128-rule limit for the interface.

address *ip_address ip_mask* **[secondary | srp-activate]**

Configures the IP address for the interface specifying the networking mask as well. *ip_address* and *ip_mask* must be entered using IPv4 dotted-decimal or IPv6 colon-separated notation.

Important: For IPv4 addresses, 31-bit subnet masks are supported per RFC 3021.

The **secondary** keyword configures a secondary IP address on the interface. This is referred to as multi-homing of the interface.
The **srp-activate** keyword activates the IP address for Interchassis Session Recovery (ICSR).

arp { arpa | timeout *seconds* **}**

Important: These keywords have been replaced by the **R_arp** command in the Global Configuration Mode. For backwards compatibility, however, these keywords are accepted as valid.

Usage

Create and manage the IP interfaces for the associated context.

Example

The following command configures the access group for the current context:

```
ip access-group sampleAccessGroup
```

```
ip address 10.2.3.4 0.0.0.128 secondary
```

The following command sets the address resolution protocol timeout.

```
ip arp timeout 1800
```

The following commands remove the associated IP address and disable ARP for the interface, respectively.

```
no ip address 10.2.3.4
```

```
no ip arp arpa
```

ip mtu

Configures the Maximum Transmission Unit (MTU) for this IP interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] ip mtu *mtu-size*

no

Deletes the MTU value.

Usage

IP MTU is supported for a normal interface and point-to-point interface (OLC ports).
The maximum MTU size allowed with an OLC port is 1600. The maximum MTU size allowed with an Ethernet port is 2048. The default MTU size is 1500.

Example

The following command sets the MTU value to *2048*.

```
ip mtu 2048
```

ip ospf authentication-key

Configures the password for authentication with neighboring Open Shortest Path First (OSPF) routers.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

ip ospf authentication-key [encrypted] password *auth_key*

no ip ospf authentication-key

no

Deletes the authentication key.

encrypted

Use this keyword if you are pasting a previously encrypted authentication key into the CLI command.

password *auth_key*

Specifies the password to use for authentication as an alphanumeric string of 1 through 16 characters entered in clear text format.

Usage

Use this command to set the authentication key used when authenticating with neighboring routers.

Example

To set the authentication key to 123abc, use the following command;

```
ip ospf authentication-key password 123abc
```

Use the following command to delete the authentication key;

```
no ip ospf authentication-key
```

ip ospf authentication-type

Configures the OSPF authentication method to be used with OSPF neighbors over the logical interface.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
ip ospf authentication-type { message-digest | null | text }

no ip ospf authentication-type { message-digest | null | text }
```

no

Disable this function.

message-digest

Uses the message digest (MD) authentication method.

null

Uses no authentication, thus disabling either MD or clear text methods.

text

Uses the clear text authentication method.

Usage

Use this command to set the type of authentication to use when authenticating with neighboring routers.

Example

To set the authentication type to use clear text, enter the following command;

```
ip ospf authentication-type text
```

ip ospf cost

Configures the cost associated with sending a packet over the OSPF logical interface.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

ip ospf cost *value*

no ip ospf cost

no

Disable this function.

value

Specifies the cost to assign to OSPF packets as an integer from 1 through 65535. Default: 10

Usage

Use this command to set the cost associated with routes from the interface.

Example

Use the following command to set the cost to *20*;

```
ip ospf cost 20
```

Use the following command to disable the cost setting;

```
no ip ospf cost
```

ip ospf intervals

Configures the interval or delay type, and the interval or delay time in seconds, for OSPF communications.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
ip ospf { dead-interval value | hello-interval value | retransmit-interval value |
transmit-delay value }

no ip ospf { dead-interval | hello-interval | retransmit-interval | transmit-delay }
```

no

Deletes the value set and returns the value to its default.

dead-interval *value*

Specifies the interval (in seconds,) that the router should wait, during which time no packets are received and after the router considers a neighboring router to be off-line. *value* must be an integer from 1 through 65535. Default: 40

hello-interval *value*

Specifies the interval (in seconds) between sending hello packets as an integer from 1 through 65535. Default: 10

retransmit-interval *value*

Specifies the interval in (seconds) between LSA (Link State Advertisement) retransmissions as an integer from 1 through 65535. Default: 5

transmit-delay *value*

Specifies the interval (in seconds) that the router should wait before transmitting a packet. *value* must be an integer from 1 through 65535. Default: 1

Usage

Use this command to set the intervals or delays for OSPF communications.

Example

To set the dead-interval to *100*, use the following command;

```
ip ospf dead-interval 100
```

To delete the setting for the dead-interval and reset the dead-interval value to its default of 40, use the following command'

```
no ip ospf dead-interval
```

ip ospf message-digest-key

Enables or disables the use of MD5-based OSPF authentication.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

ip ospf message-digest-key *key_id* **md5 [encrypted] password** *authentication_key*

no ip ospf message-digest-key *key_id*

no

Deletes the key.

message-digest-key *key_id*

Specifies the key identifier number as an integer from 1 through 255.

encrypted

Use this if you are pasting a previously encrypted authentication key into the CLI command.

password *authentication_key*

Specifies the password to use for authentication as an alphanumeric string of 1 through 16 characters entered in clear text format.

Usage

Use this command to create an authentication key that uses MD5-based OSPF authentication.

Example

To create a key with the ID of *25* and a password of *123abc*, use the following command;

```
ip ospf message-digest-key 25 md5 password 123abc
```

To delete the same key, enter the following command;

```
no ip ospf message-digest-key 25
```

ip ospf network

Configures the Open Shortest path First (OSPF) network type.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

ip ospf network { broadcast | non-broadcast | point-to-multipoint | point-to-point }

no ip ospf network

no

Disable this function.

broadcast

Sets the network type to broadcast.

non-broadcast

Sets the network type to non-broadcast multi access (NBMA).

point-to-multipoint

Sets the network type to point-to-multipoint.

point-to-point

Sets the network type to point-to-point.

Usage

Use this command to specify the OSPF network type.

Example

To set the OSPF network type to *broadcast*, enter the following command;

```
ip ospf network broadcast
```

To disable the OSPF network type, enter the following command;

```
no ip ospf network
```

ip ospf priority

Designates the OSPF router priority.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

ip ospf priority *value*

no ip ospf priority *value*

no

Disable this function.

value

Sets the priority value as an integer from 0 through 255.

Usage

Use this command to set the OSPF router priority.

Example

To set the priority to *25*, enter the following command:

```
ip ospf priority 25
```

To disable the priority, enter the following command:

```
no ip ospf priority
```

ipv6 access-group

Specifies the name of the access control list (ACL) group to assign to this interface. You can filter for either inbound or outbound traffic.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

`[ no ] ipv6 access-group` *`group name`* **`{ in | out } { priority-value`** *`priority_value`* **`}`**

`no`

Removes a previously configured access group association.

`group_name`

Specifies the name of the access group as an alphanumeric string of 1 to 79 characters.

`in`

Applies the filter to the inbound traffic.

`out`

Applies the filter to the outbound traffic.

`priority-value`

Specifies the priority of the access group as an integer from 0 to 4294967295. 0 is the highest priority. If priority-value is not specified, the priority is set to 0.
If access groups in the list have the same priority, the last one entered is used first.

Usage

Use this command to specify the ACL group to assign the interface to. Specify an ACL group name with this command.

Important: Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128-rule limit for the interface.

Example

Use the following command to associate the *`group_1`* access group with the current IPv6 profile for inbound access:

```
ipv6 access-group group_1 in 1
```

ipv6 address

Specifies the address and subnet mask.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

ipv6 address *ip_address*

ip_address

Specifies an individual host IP address to add to this host pool in IPv6 colon-separated notation.

Usage

Configures the IPv6 address and subnet mask for a specific interface.

ipv6 ospf

Enables Open Shortest Path First Version 3 (OSPFv3) functionality on this interface.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

[no] ipv6 ospf [area { *integer_value* | *ipv4-address* } | cost *cost-value* | dead-interval *dead-intrv* | hello-interval *hello-intrvl* | priority *p-value* | retransmit-interval *retx-interval* | transmit-delay *td-interval*]

no

Removes a previously configured access group association.

area { *integer_value* | *ipv4-address*

Specifies an OSPFv3 area.
decimal_value: Specifies the identification number of the area as an integer from 0 through 4294967295.
ipv4address: Specifies the IP address of the area in IPv4 dotted-decimal notation.

cost *cost-value*

Specifies a link cost as an integer from 1 through 65535. The link cost is carried in the LSA updates for each link. The cost is an arbitrary number.

dead-interval *dead-intrv*

Specifies the interval (in seconds) after which a neighbor is declared dead when no hello packets as an integer from 1 through 65535.

hello-interval *hello-intrvl*

Specifies the interval (in seconds) between hello packets that OSPFv3 sends on an interface as an integer from 1 through 65535.

priority *p-value*

Specifies the of the interface as an integer from 0 through 255.

retransmit-interval *retx-interval*

Specifies the time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPFv3 interface as an integer from 1 through 65535.

transmit-delay *td-interval*

Specifies the estimated time (in seconds) required to send a link-state update packet on the interface as an integer from 1 through 65535.

Usage

Configure an OSPFv3 interface in this context.

Example

```
ipv6 ospf area 334 cost 555 dead-interval 40 hello-interval 10 priority
10 retransmit-interval 5 transmit-delay 10
```

ipv6 router advertisement

Enables or disables the system to send IPv6 router advertisements.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ipv6 router advertisement
```

Usage

Enables sending of router advertisements on the interface. All of the pool prefixes in the context (belonging to the interface) will be advertised in the router advertisement.
The router-lifetime in the advertisement is sent as 0 to indicate to the receiver that the sender cannot be a default-router. For all the prefixes (pools), the valid and preferred lifetime are sent as default. The router-advertisement is sent every 600 seconds.
If the pool-prefix is deleted, then an router-advertisement is sent for that particular prefix with the valid and preferred time set to 0.

policy-forward

Configures the system for redirecting the HA packets to new HA during existing HA upgrade.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

policy-forward { icmp unreachable next-hop *ip address* **| unconnected-address next-system** *ip_address* **}**

no policy-forward unconnected-address

no

Deletes the policy forwarding configuration for unconnected address for the current interface.

icmp unreachable next-hop *ip address*

Specifies routing of Internet Control Message Protocol (ICMP) unreachable is required in overlapping pool configuration. *ip_address* must be an IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated notation.

unconnected-address next-system *ip address*

Specifies the IP address of the next system HA to handle processing during HA upgrade. *ip_address* must be an IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to set the redirecting policy for IP packets from an existing HA to a new HA during upgrade. To configure this command both keywords will be in separate interface.

Important: This is a customer specific command.

Example

To configure existing HA system for redirecting the HA packets to new HA during existing HA upgrade enter the following commands:

policy-forward unconnected-address next-system *ip_address*

policy-forward icmp unreachable next-hop *ip_address*

pool-share-protocol

Configures the primary or secondary system for the IP pool sharing protocol and enter IPSP configuration mode.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

```
pool-share-protocol { primary ip_address | secondary ip_address } [ mode { active |
inactive | check-config } ]

no pool-share-protocol
```

no

Deletes the IP pool sharing protocol information from the current interface.

primary *address*

On the secondary system, defines the IP address of an interface on the primary system that has identical IP pools configured for use with the IP pool sharing protocol. *ip_address* must be expressed in IP v4 dotted-decimal notation.

secondary *ip_address*

On the primary system, define the IP address of an interface on the secondary system that has identical IP pools configured for use with the IP pool sharing protocol. *ip_address* must be expressed in IP v4 dotted-decimal notation.

mode {active | inactive | check-config}

This is an optional command to manage the mode for IP pool sharing protocol for primary or secondary HA.
active: Activates the IP pool sharing protocol mode.
inactive: Inactivates the IP pool sharing protocol mode.
check-config: Verifies the IP pool sharing protocol configuration.

Usage

Use this command to set the IP address of the primary or secondary system for use with the IP pool sharing protocol and enter ipsp configuration mode. This command must be configured for an interface in each context that has IP pools configured. Refer to the System Administration and Configuration Guide for information on configuring and using the IP pool sharing protocol.

Important: Both the primary and secondary systems must be in the same subnet.

Important: For information on configuring and using IP Pool Sharing Protocol (IPSP), refer to the *Packet Data Serving Node Administration Guide*.

Important: Reserve free addresses on the primary HA for this command via the **reserved-free-percentage** command as described in the *IPSP Configuration Mode Commands* chapter of this guide.

Example

To configure a secondary system with an IP address of *192.168.100.10* for use with the IP pool sharing protocol, enter the following command:

```
pool-share-protocol secondary 192.168.100.10
```

To inactivate a secondary system with an IP address of *192.168.100.10* for use with the IP pool sharing protocol, enter the following command:

```
pool-share-protocol secondary 192.168.100.10 mode inactive
```

port-switch-on-L3-fail

Causes the line card port to which the current interface is bound to switch over to the port on the redundant line card when connectivity to the specified IP address is lost.

Product

All

Privilege

Security Administrator, Administrator

Syntax

port-switch-on-L3-fail address { *ip_address* **|** *ipv6_address* **} [minimum-switchover-period** *switch_time* **] [interval** *int_time* **] [timeout** *time_out* **] [num-retry** *number* **]**

no port-switch-on-L3-fail

no

Disable port switchover on failure.

ip_address

The IP address to monitor for connectivity, entered in IPv4 dotted-decimal or IPv6 colon-separated notation.

minimum-switchover-period *switch_time*

After a switchover occurs, another switchover cannot occur until the specified amount of time (in seconds) has elapsed. *switch_time* must be an integer from 1 through 3600. Default: 120

interval *int_time*

Specifies how often (in seconds) monitoring packets are sent to the IP address being monitored. *int_time* must be an integer from 1 through 3600. Default: 60

timeout *time_out*

Specifies how long to wait (in seconds) without a reply before resending monitoring packets to the IP address being monitored. *time_out* must be an integer from 1 through 10. Default: 3

num-retry *number*

Specifies how many times to retry sending monitor packets to the IP address being monitored before performing the switchover. *number* must be an integer from 1 through 100. Default: 5

Usage

Use this command to monitor a destination in your network to test for L3 connectivity. The destination being monitored should be reachable from both the active and standby line cards.

Example

The following command enables port switchover on connectivity failure to the IP address *192.168.10.100* using default values:

```
port-switch-on-L3-fail address 192.168.10.100
```

The following command disables port switchover on connectivity failure:

```
no port-switch-on-L3-fail
```

vlan-map

Sets a single next-hop IP address so that multiple VLANs can use a single next-hop gateway. The vlan-map is associated with a specific interface.

Product

PDSN, HA, SGSN

Privilege

Security Administrator, Administrator

Syntax

vlan-map next-hop *ip_address*

next-hop *ip_address*

Defines an IP address for the next-hop gateway in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to combine multiple VLAN links to go through a single IP address. This feature is used in conjunction with nexthop forwarding and overlapping IP pools.
After configuring the vlan-map, move to the Port Ethernet Configuration mode to attach the vlan-map to a specific VLAN.

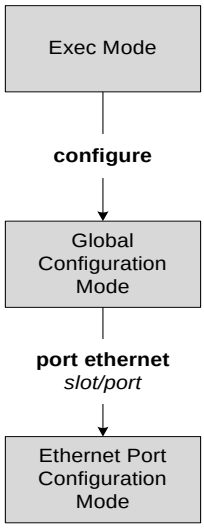
Example

The following command sets an IPv4 address for a next-hop gateway.

```
vlan-map next-hop 123.123.123.1
```

Chapter 110
Ethernet Port Configuration Mode Commands

The Ethernet Port Configuration Mode is used to create and manage Ethernet ports and their bindings between contexts.



bind interface

Configures an association (binds) between a virtual IP interface, an SS7 or Frame Relay link to a specific context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] bind interface *interface_name context_name*

no

Indicates the virtual interface specified is to be unbound from the context.

interface_name

Specifies the name of the virtual interface to be bound to the context as an alphanumeric string of 1 through 79 characters.

context_name

Specifies the name of the context to be bound to the virtual port. *context_name* must refer to a previously configured context.

Usage

Bind an interface to a context to allow the context to provide service.

Example

```
bind interface sampleVirtual sampleContext

no bind interface sampleVirtual sampleContext
```

default

Restores the speed and communication mode of the default interface for the specified context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
default { flow-control | link-aggregation { lacp | redundancy } | medium | preferred slot
| threshold { high-activity | monitoring | rx-utilization | tx-utilization } }
```

flow-control

Restores the default behavior to advertise symmetric flow control.

link-aggregation { lacp | redundancy }

Restores the default values for link-aggregation as follows:

- **lacp**: Active – sends out LACP packets periodically.
- **redundancy**: Standard – treats all cards in the group as one group.

medium

Restores the default values for the medium options as follows:

- SPIO and fast ethernet line cards: auto
- Gigabit ethernet line card: auto

preferred slot

Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a port switch to command to return service to the original port.

threshold { high-activity | monitoring | rx-utilization | tx-utilization }

Restores the specified port-level threshold parameters to its default value(s). The possible values are:

- **high-activity**: High port activity threshold settings. Default: 50 percent
- **monitoring**: Threshold monitoring configuration settings. Default: Disabled
- **rx-utilization**: Receive port utilization threshold settings. Default: 80 percent
- **tx-utilization**: Transmit port utilization threshold settings. Default: 80 percent

Usage

Restores port-level parameters to their default values.

Example

```
default medium
```

description

Sets the port descriptive text.

Product

All

Privilege

Security Administrator, Administrator

Syntax

description *text*

no description

no

Clears the description for the port.

text

Specifies the descriptive text as an alphanumeric string of 1 to 79 characters.

Usage

The description should provide useful information on the port's primary function, services, end users, etc.

Example

```
description samplePortDescriptiveText

description "This is a sample description"
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

fault-unidirect-mode

Configures the unidirectional mode that generates fault messages for the connection's peer when local faults are detected and remote faults are received.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] fault-unidirect-mode ( clause-46 | clause-66 }
```

no fault-unidirect-mode

Disables fault message generation.

(clause-46 | clause-66 }

clause-46: On local fault reception, continuous remote faults are sent. On remote fault reception, continuous idles are sent. [IEEE 802.3, Clause 46, Reconciliation Sublayer (RS) and 10 Gigabit Media Independent Interface (XGMII)]
clause-66: On local fault reception, frame transmit is continued, remote fault indication is sent during Inter-Frame Gap (IFG). On remote fault reception, frame transmit is continued. [IEEE 802.3, Clause 66, Extensions of the 10 Gb/s Reconciliation Sublayer (RS), 100BASE-X PHY, and 1000BASE-X PHY for unidirectional transport]

Usage

Configure the unidirectional mode that generates fault messages for the connection's peer when local faults are detected and remote faults are received.

Example

After flow control has been disabled, use the following command to enable flow control:

```
fault-unidirect-mode clause-46
```

flow-control

Enables and disables flow control on the Quad Gig-E line card (QGLC).

Product

PDSN, SGSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] flow-control
```

no

Disables flow control on the specified port.

Usage

Flow control is enabled by default on the QGLC and can be disabled using the **no** command on a per-port basis. This command does not work on the Fast Ethernet Line Card (FELC), Gigabit Ethernet Line Card (GELC/GLC2) or 10 GigE Line Card (XGLC) which do not support flow control.

Example

After flow control has been disabled, use the following command to enable flow control:

```
flow-control
```

ingress-mode

Labels this port as an ingress port.

Product

IPSG

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ingress-mode
```

no

Disables ingress port tag.

Usage

Use this command to label this port in order for the session manager to recognize the interface from which IP data packets are being received. This command should be used in single context configurations. In single context configurations, the ingress port can only be identified if labeled.

link-aggregation

Aggregates ports on a Quad Gig-E line card (QGLC) or 10 Gig-E line card (XGLC) and set related parameters in accordance IEEE 802.3ad.

Product

WiMAX, PDSN, HA, FA, GGSN, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
link-aggregation { distribution { block | random | rotate | simple } | lacp { active |
passive } [ rate { auto | fast | slow } ] [ timeout { long | short } ] | master { global
group group_number | group group_number | local group group_number } | member { global
group group_number | group group_number | local group group_number } | redundancy {
standard | switched } [ hold-time sec ] [ preferred slot { card_number | none } ] |
toggle-link }

no link-aggregation [ toggle-link ]

default link-aggregation { distribution | lacp | redundancy | toggle-link }
```

distribution { block | random | rotate | simple }

Configures link aggregation distribution and controls how a Link Aggregation Group (LAG) hash map is generated. This method is required for Equal Cost Multi-Path (ECMP) routing over LAG. Set this option on the master port for use with the whole group. The following list defines the distribution options (assuming port index 0,1,2,3 were selected.
block: Blocks of the same port index (Example: 0000111122223333)
random: Based on pseudo random number
rotate: Repetition of rotated port index (Example: 0123123023013012…)
simple: Repetition of all selected port indexes (Example: 0123012301230123…)

lacp { active | passive }

Configures the Link Aggregation Control Protocol (LACP). Set this option on the master port for use with the whole group.
active mode sends out LACP packets periodically. (Default)
passive mode only responds to LACP packets received.

rate { auto | fast | slow }

Configures the rate at which the LACP sends packets.
auto: rate is controlled by the peer
fast: 1 seconds
slow: 30 seconds (Default)

timeout { long | short }

Configures LACP timeout events. Set this option on the master port for use with the whole group.
long: Set LACP to long timeout
short: Set LACP to short timeout

master { global group *group_number* **| group** *group_number* **| local group** *group_number* **}**

This command creates the Master port for the aggregated group.
global: Set group global across slots.
group *group_number*: Set link aggregation group number. *group_number* must be an integer between 1 and 1023.
local: Set group local within same slot.

member { global group *group_number* **| group** *group_number* **| local group** *group_number* **}**

This command makes the port a member of the aggregated group.
global: Set group global across slots.
group *group_number*: Set link aggregation group number. *group_number* must be an integer from 1 through 1023.
local: Set group local within same slot.

redundancy { standard | switched } [hold-time *sec* **] [preferred slot {** *card_number* **| none }]**

Connects top and bottom QGLCs and side-by-side XGLCs to different switches. The master port must be set to make this effective for the group.
standard: Treats all cards in the group as one group. (Default)
switched: Assumes cards are connected to different switches.
hold-time *sec*: Sets the amount of time to hold (in seconds) before switching between cards. Applies to standard and switched modes. *sec* must be an integer from 0 through 3600. Default: 10
preferred slot*card_number*: Specifies revertive/non-revertive preference including preferred slot for standard LAG for two switches. Applies to standard and switched modes. *card_number* is an integer between 1 and 48
none: Specifies no preferred slot.

toggle-link

Set to toggle link on port switch.

default

Restores the default values.

no

This command deletes the Ethernet port from any group it might be in. If the port was the Master of a group, the whole group would be deleted.

Usage

Configure from one to four ports on a QGLC (vertical aggregation) or the single port on XGLCs (horizontal aggregation) to be in an aggregation group on the chassis that links to an aggregation group on a remote switch. Very large files can be downloaded across all ports in a group, which makes for a faster download when compared to serial downloads over a single link. For additional information, refer to the *System Administration Guide*.

Example

The following example configures the port to be the Master for Group *2*:

```
link aggregation master group 2
```

media

Configures the port interface type.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
media { rj45 | sfp }
```

{ rj45 | sfp}

rj45: Sets the physical interface to copper RJ-45 connectors.
sfp: Sets the physical interface connection to optical Small Form Factor (SFP) gigabit via an SFP transceiver.

Usage

Set the media option when the physical cabling interface is changed.

Example

The following commands are entered one-at-a-time to set the physical interface to RJ-45 and SFP:

```
media rj45

media sfp
```

medium

Configures the port speed and communication mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
medium { auto | speed { 10 | 100 | 1000 | 10000 } duplex { full | half } }
```

{ auto | speed { 10 | 100 | 1000 | 10000 } duplex { full | half } }

Default: **auto**
Optionally sets the speed of the interface and the communication mode.
auto: configures the interface to auto negotiate the interface speed.
speed { 10 | 100 | 1000 | 10000 }: specifies the speed to use at all times.
duplex { full | half }: sets the communication mode of the interface to either **full** or **half** duplex.

Important: Ethernet networking rules dictate that if a device whose interface is configured to auto-negotiate is communicating with a device that is manually configured to support full duplex, the first device will negotiate to the manually configured speed of the second device but will only communicate in half duplex mode.

Usage

Set the medium options when the physical interface changes.

Example

The following configures the port's speed and communication mode to be auto negotiated.

```
medium auto
```

The following command configures the port's interface speed to gigabit with full duplex communication.

```
medium speed 1000 duplex full
```

preferred slot

Assigns revertive or non-revertive control to port redundancy auto-recovery.

Default: non-revertive operation

Product

PDSN, FA, HA, SGSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] preferred slot slot#
```

no

Disables revertive or auto-recovery operation for the selected port.

preferred slot *slot#*

Identifies the physical chassis slot where the line card or SPIO card is installed.

Usage

This command enables or disables revertive port redundancy, wherein after a port failover, when the original port is restored to service (such as link up) the system will return service to that port automatically.
Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a **port switch** to command to return service to the original port.
This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual line or SPIO cards. For example, ports 1 through 4 could be configured as "preferred" on the LC in slot 17 while ports 5 through 8 are "preferred" on the LC in slot 33. In this scenario, both LCs would be in an Active operational state while still providing LC and port redundancy for the other.

Important: This command is not supported on all platforms.

Example

```
preferred slot 17
```

shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, the port is enabled with the use of the **no** keyword.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] shutdown
```

no

Enables the port and places it in service.

Usage

Shut down a port prior to re-cabling and/or other maintenance activities.
This command is necessary to bring a port into service by enabling it via the **no** keyword.

Example

Use the following command to disable the port:

```
shutdown
```

Use the following command to enable the port for service:

```
no shutdown
```

snmp trap link-status

Enables or disables the generation of an SNMP trap for link status changes.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] snmp trap link-status
```

no

Disables the sending of traps for link status changes.

Usage

Enable link status change traps when a monitoring facility can use the information or if there are troubleshooting activities in progress.

Example

Use the following command to disable sending of traps:

```
no snmp trap link-status
```

srp virtual-mac-address

Configures the Standby Router Protocol (SRP) virtual MAC address for the port.

Product

All

Privilege

Security Administrator, Administrator

Syntax

srp virtual-mac-address *MAC_Address*

no srp virtual-mac-address

no

Disables the SRP virtual MAC addressing for Ethernet ports. The block of virtual MAC addresses is not saved.

MAC_Address

Enables SRP virtual addressing for the specified MAC address.

Usage

The SRP virtual MAC address is applied to the port when the chassis is in SRP ACTIVE state. The default is **no srp virtual-mac-address**.

Important: This command is not supported on all platforms.

Example

Use the following command to enable the SRP's virtual MAC addressing:

srp virtual-mac-address *MAC_Address*

threshold high-activity

Configures thresholds for high port activity for the port.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold high-activity *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Specifies the high threshold high port activity percentage that must be met or exceeded within the polling interval to generate an alert or alarm. The percentage is expressed as an integer from 0 through 100. Default: 50

clear

Allows the configuration of the low threshold.

low_thresh

Specifies the low threshold high port activity percentage that maintains a previously generated alarm condition. If the activity percentage falls below the low threshold within the polling interval, a clear alarm will be generated. The percentage is expressed as an integer from 0 through 100. Default: 50

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

High port activity thresholds generate alerts or alarms based on the utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis.
Alerts or alarms are triggered for high port activity based on the following rules:

- **Enter condition**: Actual percent utilization of a port is greater than High Threshold.
- **Clear condition**: Actual percent utilization of a port is less than Low Threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command in the *Global Configuration Mode Commands* chapter to configure the polling interval and the **threshold monitoring** command in this chapter to enable thresholding for this value.

Example

The following command configures a high port utilization threshold percent of *70* and a low threshold percent of *50* for a system using the Alarm thresholding model:

```
threshold high-activity 70 clear 50
```

threshold monitoring

Enables or disables thresholding for port-level values.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] threshold monitoring
```

no

Disables threshold monitoring for port-level values. This is the default setting.

Usage

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (such as high-activity) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. Thresholding helps identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the *SNMP MIB Reference*. The generation of specific SNMP traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.
- **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.
- **Alarm System**: High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists and/or a condition clear alarm is generated.

"Outstanding" alarms are reported to through the system's alarm subsystem and are viewable through the system's CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

Table 18. Thresholding Reporting Mechanisms by Model

Model	SNMP Traps	Logs	Alarm System
Alert	X	X	
Alarm	X	X	X

This command enables thresholding for port-level values. Refer to the **threshold high-activity**, **threshold rx-utilization**, and **threshold tx-utilization** commands in this chapter for information on configuring these values. In addition, refer to the **threshold poll** command in the *Global*

Configuration Mode Commands chapter for information on configuring the polling interval over which these values are monitored.

threshold rx-utilization

Configures thresholds for receive port utilization.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold rx-utilization *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Specifies the high threshold receive port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. The percentage is expressed as an integer from 0 through 100. Default: 80

clear

Allows the configuration of the low threshold.

low_thresh

Specifies the low threshold receive port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a Clear Alarm will be generated. The percentage is expressed as an integer from 0 through 100. Default: 80

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis.

Important: Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive **or** transmit utilization threshold be configured.

Alerts or alarms are triggered for receive port utilization based on the following rules:

- **Enter condition**: Actual percent utilization of a port for received data is greater than High Threshold
- **Clear condition**: Actual percent utilization of a port for received data is less than Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command in the *Global Configuration Mode Commands* chapter to configure the polling interval and the **threshold monitoring** command in this chapter to enable thresholding for this value.

Example

The following command configures a receive port high utilization threshold percent of *70* and a low threshold percent of *50* for an system using the Alarm thresholding model:

```
threshold rx-utilization 70 clear 50
```

threshold tx-utilization

Configures thresholds for transmit port utilization.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold tx-utilization *high_thresh* **[clear** *low_thresh* **]**

high_thresh

The high threshold transmit port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. The percentage is expressed as an integer from 0 through 100. Default: 80

clear

Allows the configuration of the low threshold.

low_thresh

The low threshold transmit port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated. The percentage is expressed as an integer from 0 through 100. Default: 80

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis.

Important: Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive **or** transmit utilization threshold be configured.

Alerts or alarms are triggered for transmit port utilization based on the following rules:

- **Enter condition**: Actual percent utilization of a port for transmit data is greater than High Threshold
- **Clear condition**: Actual percent utilization of a port for transmit data is less than Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command in the *Global Configuration Mode Commands* chapter to configure the polling interval and the **threshold monitoring** command in this chapter to enable thresholding for this value.

Example

The following command configures a transmit port high utilization threshold percent of *70* and a low threshold of *50* for an system using the Alarm thresholding model:

```
threshold tx-utilization 70 clear 50
```

vlan

Creates or deletes a VLAN tag and enters VLAN Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

vlan *tag* **[inline-process] [subscriber-vlan] [-noconfirm]**

no vlan *tag*

no

Deletes the VLAN with the specified tag.

tag

Specifies a tag that identifies the VLAN an integer from 1 through 4095. The tag must be unique and not used by any other VLANs on any other ports in the system.

inline-process

Do not use this restricted keyword. It sets this VLAN for special processing for packets received from an external inline server.

subscriber-vlan

Designates the VLAN type as a subscriber VLAN. This keyword must be specified if the VLAN is to be associated with specific subscribers. Refer to the **ip vlan** command in the *Subscriber Configuration Mode* chapter of this reference for additional information on Subscriber-VLAN associations.

Important: To maintain optimal performance, this keyword should not be specified for VLANs that are not to be associated with subscribers.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Virtual LANs (VLANs) provide greater flexibility in the configuration and use of contexts and services. They are configured as “tags” on a per-port basis and allow more complex configurations to be implemented. The VLAN tag allows a single physical port to be bound to multiple logical interfaces that can be configured in different contexts. Therefore, each Ethernet port can be viewed as containing many logical ports when VLAN tags are employed.

Important: VLANs are supported in conjunction with ports on the Ethernet 10/100 and Ethernet 1000 line cards, as well as on the four-port Quad Gig-E Line Card (QGLC) and the single port 10 GigE Line Card (XGLC). (VLAN tagging is not supported for SPIO ports.) The system supports the configuration of VLANs as follows:

Important: Ethernet 1000 Line Card/QGLC: 1024 VLANs per card. QGLC supports 511 VLANs per port.

Important: Ethernet 10/100 Line Card: Maximum of 256 VLANs per port and a maximum of 1016 VLANs per Line Card. (VLANs on all the ports of a single 10/100 Line Card can not add up to more than 1016.)

Important: In order to change the type (using/removing the **subscriber-vlan** keyword) for VLANs that are already configured, the VLAN must first be deleted and then reconfigured as desired.

Example

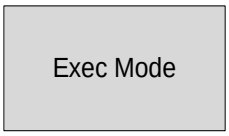
The following example creates a VLAN and assign it the tag of *100*:

```
vlan 100
```

Chapter 111
Exec Mode Commands (A-C)

This section includes the commands **aaa test** through **crypto-group**.

The Exec Mode is the initial entry point into the command line interface system. Exec mode commands are useful in troubleshooting and basic system monitoring.



aaa test

Tests Authentication, Authorization and Accounting (AAA) functionality between this system and a remote server.

Product

PDSN, HA, GGSN, SGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator

Syntax

aaa test { accounting username *user_name* **| authenticate** *user_name password* **| session** *user_name password* **}**

accounting username *user_name*

Tests RADIUS or GTPP accounting functionality for the specified user.
user_name must be the name of a user configured on the RADIUS or CFG server.

Important: GTPP is used only in conjunction with the GGSN or SGSN product.

authenticate *user_name password*

Tests RADIUS authentication functionality for the specified user.
user_name is the name of a user configured on the RADIUS server. *password* is the user's password.

session *user_name password*

Tests both RADIUS authentication and RADIUS or GTPP accounting functionality for the specified user.
user_name is the name of a user configured on the RADIUS server. *password* is the user's password.

Important: GTPP is used only in conjunction with the GGSN or SGSN product.

Usage

This command is used to test RADIUS-based authentication and RADIUS or GTPP accounting. This command may be useful for diagnosing problems with subscribers and access to the system and/or billing data.

Example

The following command verifies accounting for a user named *user1*:

```
aaa test accounting username user1
```

The following command tests authentication for a user named *user1* with the password *abc123*:

```
aaa test authentication user1 abc123
```

The following command tests both accounting and authentication for the user named *user1* with the password *abc123*:

```
aaa test session user1 abc123
```

active-charging service

Creates an active charging service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator

Syntax

active-charging service *ecs_service_name* **[-noconfirm]**

active-charging service *ecs_service_name*

Specifies name of the active charging service as an alphanumeric string of 1 through 15 characters.
If the named service does not exist, it is created and the CLI mode changes to the ACS Configuration Mode wherein the service can be configured.
If the named service already exists, the CLI mode changes to the ACS Configuration mode wherein the specified active charging service can be configured.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to create an active charging service in the system. This command can be used directly in Exec Mode after issuing the **require active-charging** command in the Global Configuration Mode. This command allows an operator (rather than security administrators and administrators) to configure the ACS functionality only.

Important: Operators need special CLI privilege for ACS functionality to be able to use this CLI command.

Example

The following command creates an active charging service named *test*:

```
active-charging service test
```

alarm

Disables the internal audible alarm on the system management card.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
alarm cutoff
```

Usage

Alarm cutoff disables the audible alarm. The alarm may be enabled following this command if an event within the system results in the audible alarm being enabled.

Example

```
alarm cutoff
```

aps

Allows the operator to perform SONET Automatic Protection Switching (APS) administrative operations.

Important: Use of this command is limited to the OLC2 and the CLC2 line cards.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

aps { clear *slot#/port#* **| exercise** *slot#/port#* **| lockout** *slot#/port#* **| switch { force | manual }** *slot#/port#* **}**

clear *slot#/port#*

Clears the last switch command on the specified channelized port.
slot#/port# is the CLC2/OLC2 slot number (valid range is 17 - 48) and appropriate port number (CLC2 valid range is 1 - 4; OLC2 valid value is 1).

exercise *slot#/port#*

Tests the APS protocol on line connected to port.
slot#/port# is the CLC2/OLC2 slot number (valid range is 17 - 48) and appropriate port number (CLC2 valid range is 1 - 4; OLC2 valid value is 1)

lockout *slot#/port#*

Prevents the working port from switching to the protection port.
slot#/port# is the CLC2/OLC2 slot number (valid range is 17 - 48) and appropriate port number (CLC2 valid range is 1 - 4; OLC2 valid value is 1)

switch { force | manual } *slot#/port#*

Switch to either the working port or the protection port:

- **force**: Forces a switch of ports, even if there is an active alarm state.
- **manual**: Implements a switch of ports if there are no active alarms.

slot#/port# is the CLC2/OLC2 slot number (valid range is 17 - 48) and appropriate port number (CLC2 valid range is 1 - 4; OLC2 valid value is 1)

Usage

This command allows an operator to perform administrative/maintenance APS tasks such as testing the APS protocol, switching the working port to the protection port, and locking out the switching function.

Example

The following command starts an APS protocol test on port 2 of card 27:

```
aps exercise 27/2
```

autoconfirm

Enables or disables confirmation for certain commands. This command affects the current CLI session only.

Important: Use the **autoconfirm** command in the Global Configuration Mode to change the behavior for all future CLI sessions.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
autoconfirm

no autoconfirm
```

Usage

When **autoconfirm** is enabled, certain commands ask you to answer yes or no to confirm that you want to execute the command. When **autoconfirm** is disabled, the confirmation questions never appear. Disabling **autoconfirm** is active for the current session only.
By default **autoconfirm** is enabled.

Example

The following command enables command confirmation:

```
autoconfirm
```

The following command disables command confirmation for the duration of the current CLI session:

```
no autoconfirm
```

bulkstats force

Manages the collection and delivery of system statistics (bulkstats) to the configured server.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
bulkstats force { gather | transfer }
```

bulkstats force gather

Immediately collects the system statistics.

bulkstats force transfer

Immediately sends the currently collected statistics to the configured server.

Usage

When the current system statistics are desired immediately as opposed to the normal scheduled collection and delivery intervals issue this command.
Troubleshooting the system may require the review of statistics at times when the scheduled delivery is not timely.

Example

The following causes the chassis to immediately collect system statistics. This would be in anticipation of a transfer command.

```
bulkstats force gather
```

The following command causes the chassis to immediately send all collected statistics to the configured server.

```
bulkstats force transfer
```

call-home send

Manages how Cisco Smart Call Home messages are sent to alert groups.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

call-home send alert-group { configuration profile *profile name* **| inventory profile** *profile name* **}**

configuration profile *profile name*

Sends configuration messages to the previously defined profile, expressed as an alphanumeric string of 1 through 31 characters.

inventory profile *profile name*

Sends inventory messages to the previously defined profile, expressed as an alphanumeric string of 1 through 31 characters.

Usage

Use this command to send specified alert-group call-home message from the CLI to all profiles subscribed to the specified alert group, or to a specified profile which does not need to be subscribed to the specified alert-group. For additional information, refer to the *Call-Home Configuration Mode Commands* and *Call-Home Profile Configuration Mode Commands* chapters.

Example

The following command sets the system to send configuration related call-home messages to the profile named *Profile1*.

```
call-home send alert-group configuration profile Profile1
```

call-home test

Sends a test Smart Call Home event message to a specified profile.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

call-home test message { *test_message_content* **| profile** *profile name* **}**

call-home test message message *test_message_content*

Defines the message to send to the defined profile as an alphanumeric string of 1 through 128 characters.

profile *profile_name*

Specifies the previously defined profile to which the message will be sent, expressed as an alphanumeric string of 1 through 31 characters.

Usage

Use this command to send test call-home messages from the CLI to a specified profile. If a message is not specified, the system sends out a default message.

Example

The following command sets the system to send a test call-home message *Test_Message_1* to the profile named *Profile1*.

```
call-home test message Test_Message_1 profile Profile1
```

card busy-out

Moves processes from the source packet processing card to the destination packet processing card, or disables the packet processing card from accepting any new calls. When busy-out is enabled, the packet processing card stops receiving new calls but continues to process calls until they are completed. The command prompt is returned once the command is initiated. The busy-out procedure is completed in background.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
card busy-out { migrate from src_slot to dst_slot } [ -noconfirm ]

no card busy-out
```

no card busy-out

Disables busy-out. The packet processing card is re-enabled to accept new calls.

migrate from *src_slot* **to** *dst_slot*

Moves processes from the specified source packet processing card to the specified destination packet processing card. The command prompt is returned once the command is initiated. The card migration is completed in background.
src_slot indicates the source slot number of the card from which processes will be migrated. *dst_slot* indicates the destination slot number of the card to which processes will be migrated.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Migrating a packet processing card changes the active/standby status of a packet processing card. This results in the active sessions/processes being moved to the newly active card. This is useful when there is a maintenance activity on the active card which requires removing the card from service.
The destination slot specified must contain a packet processing card which is in the standby state for the command to complete successfully.

Caution: Be cautious when executing this command. Depending on the number of active sessions being migrated, some subscribers may experience service interruptions.

Using busy-out to refuse new calls on a packet processing card allows you to take a card out of service without any interruptions to the end user. An individual system can be taken completely out of service gracefully by enabling busy-out on all packet processing cards and waiting for current calls to complete. The **show card info** command shows if busy-out is enabled.

Important: When a packet processing card fails, is migrated, or is restarted for any reason, busy-out is reset to disabled, the default behavior.

Important: This command is not supported on all platforms.

Example

The following command migrates the active processes from the packet processing card in slot *12* to the card in slot *14*. This command executes after you provide confirmation of the request.

```
card migrate from 12 to 14
```

```
card migrate from 1 to 8
```

The following command sets the packet processing card in slot 1 to stop accepting new calls:

```
card busy-out 1
```

card halt

Halts all StarOS processes on a card. A **card reboot** command must be issued to bring the card back into service after it is halted.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

card halt *slot_num* **[-force] [-noconfirm]**

slot_num

Indicates the slot number of the card of interest.

-force

Over-rides any warnings to force the card to be halted.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Halt a card to stop the card for maintenance or emergency situations.

Caution: Caution should be taken in using this command. Halting a card which has no redundant card available may cause a service interruption and loss of active sessions.

Caution: The **-force** and **-noconfirm** options should only be used concurrently by experienced users as this will cause an immediate halt regardless of warnings and no confirmation from the user.

Important: This command is not supported on all platforms.

Example

The following command temporarily stops the card in slot 1.

```
card halt 1
```

The following commands force the card to halt and indicate no confirmation is to take place, respectively.

```
card halt 1 -force -noconfirm
```

```
card halt 1 -noconfirm
```

card migrate

Migrates StarOS processes from an active packet processing card to a standby packet processing card.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

card migrate from *src_slot* **to** *dst_slot* **[-noconfirm]**

src_slot

Indicates the slot number of the packet processing card from which processes will be migrated. **The packet processing card in this slot must be in Active mode.**

dst_slot

Indicates the slot number of the packet processing card to which processes will be migrated.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

This command allows an operator to move processes from an active to a standby packet processing card.

Example

The following will cause processes currently running on the card in slot 8 to migrate to the standby card in slot 9. The migration will not occur if any warnings are generated.

```
card migrate from 8 to 9
```

card reboot

Resets of the target card. Rebooting a packet processing or line card will result in the card downloading the image from the active system management card.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

card reboot *target_slot* **[-force] [-noconfirm]**

card reboot *target_slot*

Initiates a reboot of the card in the specified the slot number.

-force

Indicates that the reboot is to take place ignoring any state or usage warnings that might be generated.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

A reboot is used to reset the card and receive a new download. This may be useful when a card is not responding or when it is necessary to cause the card to reload its image and restart.

Important: Caution should be taken in using this command. Rebooting a card which has no redundant card available may cause a service interruption and loss of active sessions.

Caution: The **-force** and **-noconfirm** options should only be used concurrently by experienced users as this will cause an immediate reboot regardless of warnings and no confirmation from the user.

Important: This command is not supported on all platforms.

Example

The following will cause the card in slot 8 to reboot without any confirmation from the user. The card will not reboot if there are any warnings generated.

```
card reboot 8 -noconfirm
```

The following command will cause the card in slot 8 to reboot regardless of any warnings. The user must provide confirmation prior to this command executing.

```
card reboot 8 -force
```

The following command will cause the card in slot 8 to reboot regardless of any warnings with no additional user confirmation.

```
card reboot 8 -force -noconfirm
```

card restart

Performs a soft-reset of the target card causing all application processes to restart.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
card restart target_slot [ -force ] [ -noconfirm ]
```

card restart *target_slot*

Initiates a restart of the card in the specified slot number.

-force

Indicates the restart is to take place ignoring any state or usage warnings that might be generated.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Restarting a card may be useful when a card is not performing as expected (performance drop, increased response delays, etc.). A restart may be preferred to a reboot as the card becomes available in less time than a reboot.
When this command is issued for an active card, the user is prompted for confirmation unless the **-force** and/or **-noconfirm** keywords are used. Because the reboot of standby or redundant cards is non-service impacting, the reboot proceeds immediately after the command execution without user confirmation.

Important: Caution should be taken in using this command. Restarting a card which has no redundant card available may cause a service interruption and loss of active sessions.

Important: This command is not supported on all platforms.

Caution: The **-force** and **-noconfirm** options should only be used concurrently by experienced users as this will cause an immediate restart regardless of warnings and no confirmation from the user.

Example

The following will cause the card in slot 8 to restart without any confirmation from the user. The card will not reboot if there are any warnings generated.

```
card restart 8 -noconfirm
```

The following command will cause the card in slot 8 to restart regardless of any warnings. The user must provide confirmation prior to this command executing.

```
card restart 8 -force
```

The following command will cause the card in slot 8 to restart regardless of any warnings with no additional user confirmation.

```
card restart 8 -force -noconfirm
```

card switch

Manages card pairs and their active/standby status.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
card switch { from target_slot | to target_slot } [ -noconfirm ]
```

from *target_slot*

Specifies the slot number of a currently active card that is to be switched. The slot number must be valid and contain a card in active mode.

to *target_slot*

Specifies the slot number of a standby card which is to become the active card. The slot number must be valid and contain a card in standby.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Card switch-overs change the active/standby status of a card. This is useful when there is a maintenance activity on the active card which requires removing the card from service.

Caution: Caution should be taken in using this command. Depending on the amount of bandwidth/traffic being switched, some subscribers may experience service interruptions.

Important: This command is not supported on all platforms.

Example

The following command switches the active/standby status of the line cards in slots 17 and 18. This command only executes after you provide confirmation of the request.

```
card switch from 17 to 18
```

card upgrade

Upgrades the programmable memory on a card.

Product

All

Privilege

Security Administrator, Administrator

Syntax

card upgrade *slot_number*[**-noconfirm**]

slot_number

The slot number of the card to be upgraded, from 1 through 16.

--noconfirm

Executes the command without any additional prompt and confirmation from the user.

Caution: Use this command only if instructed by or working with Technical Assistance Center personnel.

Usage

You can only initiate an upgrade if:

- there is no migration occurring,
- the card is active or standby,
- there is no online upgrade in progress.

Important: The following operations are not allowed while a card is upgrading: change edc requirement (config), change card [no] shutdown (config), change card active (config), change card redundancy (config), card halt (exec), card reboot (exec), start an online upgrade.

Important: Level unlock operations are ignored while a card is upgrading.

Important: This command is not supported on all platforms.

Example

The following command initiates a packet processing card upgrade on slot number 10:

```
card upgrade 10
```

cdr-push

Initiates a manual push of CDR files to a configured URL or Local - External Storage System (L-ESS).

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

cdr-push { all | local-filename *file_name* **}**

all

Pushes all CDR files to the configured URL.

local-filename *file_name*

Pushes only the specified file to the configured URL. *file_name* must define the absolute path of a local file name to push, expressed as an alphanumeric string of 1 through 1023 characters.

Usage

Use this command to manually push CDR files to the a configured URL or L-ESS.
For information on configuring the L-ESS, see the **cdr** command in the *EDR Module Configuration Mode Commands* and the *UDR Module Configuration Mode Commands* chapters.
Run this command only from the local context. If you are in any other context, you will see this failure message: “Failure: Manual PUSH of CDRs supported only in the local context”

Example

The following command pushes all CDR files to the URL:

```
cdr-push all
```

chassis

Identifies the chassis that can encrypt and decrypt encrypted passwords in the configuration file. If two or more chassis are configured with the same chassis key value, the encrypted passwords can be decrypted by any of the chassis sharing the same chassis key value. As a corollary to this, a chassis key value will not be able to decrypt the passwords that were encrypted using a different chassis key value.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] chassis { key value *key_string* **| keycheck** *key_string* **}**

no chassis key

Resets the chassis key to the factory default value. The factory default value is unique to the chassis. Once this command is executed, the **chassis key value** command can be used to change the default chassis key.

key value *key_string*

Specifies the chassis key value as an alphanumeric string of 1 through 16 characters.

The chassis key value is stored as a one-way encrypted value, much like a password. It is never displayed in its plain-text form.

keycheck *key_string*

Generates a one-way encrypted key value based on the entered alphanumeric string of 1 through 16 characters.

The generated encrypted key value is compared against the encrypted key value of the previously entered chassis key value. If the encrypted values match, then the command succeeds and key check passes. If the comparison fails, a message is displayed indicating that the key check has failed. Note that if the default chassis key (no chassis key) is currently being used, this key check will always fail since there will be no chassis key value to compare against.

Usage

Establish multiple, unique chassis keys to encrypt and decrypt passwords in configuration files.

Example

The following command generates a one-way encrypted key based on the string *tewks367*.

```
chassis key value tewks367
```

clear aaa

Clears all Authentication, Authorization and Accounting (AAA) statistics in the current context.

Product

PDSN, GGSN, ASN-GW, P-GW

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear aaa local counters
```

Usage

Clearing the AAA statistics may be useful when monitoring the statistics manually. Clearing resets the counters to zero.
The keyword **local** is not intended to imply the local context defined for all systems. Rather, it indicates the statistics within the current context are to be cleared.

Example

The following command zeroes out all the AAA statistics in the current context.

```
clear aaa local counters
```

clear active-charging analyzer statistics

Clears protocol analyzer statistics.

Product

ACS

Privilege

Security Administrator, Administrator, Operator

Syntax

clear active-charging analyzer statistics [name *protocol_name* **] [| { grep** *grep_options* **| more }]**

---

name *protocol_name*

Clears statistics for the specified protocol analyzer.
If this keyword is not specified all statistics are cleared.
protocol_name must be one of the following:

- **dns**
- **file-transfer**
- **ftp**
- **http**
- **icmp**
- **icmpv6**
- **imap**
- **ip**
- **ipv6**
- **mms**
- **p2p [application]**: Peer-to-peer analyzer. The supported applications are:
  - **actsync**
  - **aimini**
  - **antsp2p**
  - **applejuice**
  - **ares**
  - **armagettron**
  - **battlefld**
  - **bittorrent**
  - **blackberry**
  - **citrix**
  - **clubpenguin**
  - **crossfire**

- **ddlink**
- **directconnect**
- **dofus**
- **edonkey**
- **facebook**
- **facetime**

> ***Important:*** The **facetime** protocol is available only in releases 9.0 and 11.0. This protocol is not available in release 10.0.

- **fasttrack**
- **feidian**
- **fiesta**
- **filetopia**
- **florensia**
- **freenet**
- **fring**
- **funshion**
- **gadu_gadu**
- **gamekit**

> ***Important:*** The **gamekit** protocol is available only in releases 9.0 and 11.0. This protocol is not available in release 10.0.

- **gmail**
- **gnutella**
- **gtalk**
- **guildwars**
- **halflife2**
- **hamachivpn**
- **iax**
- **icecast**
- **imesh**
- **imo**
- **iptv**
- **irc**
- **isakmp**
- **iskoot**
- **itunes**

- **jabber**
- **kontiki**
- **manolito**
- **maplestory**
- **meebo**
- **mgcp**
- **msn**
- **mute**
- **mypeople**
- **myspace**
- **netmotion**
- **nimbuzz**
- **octoshape**
- **off**
- **ogg**
- **oovoo**
- **openft**
- **openvpn**
- **orb**
- **oscar**
- **paltalk**
- **pando**
- **pandora**
- **popo**
- **pplive**
- **ppstream**
- **ps3**
- **qq**
- **qqgame**
- **qqlive**
- **quake**
- **quicktime**
- **rdp**
- **rdt**
- **rfactor**
- **rmstream**
- **scydo**

- **secondlife**
- **shoutcast**
- **skinny**
- **skype**
- **slingbox**
- **sopcast**
- **soulseek**
- **splashfighter**
- **spotify**
- **ssdp**
- **stealthnet**
- **steam**
- **stun**
- **tango**
- **teamspeak**
- **teamviewer**
- **thunder**
- **tor**
- **truphone**
- **tunnelvoice**
- **tvants**
- **tvuplayer**
- **twitter**
- **ultrabac**
- **usenet**
- **uusee**
- **veohtv**
- **viber**
- **vpnx**
- **vtun**
- **warcft3**
- **whatsapp**
- **wii**
- **winmx**
- **winny**
- **wmstream**
- **wofkungfu**

- **wofwarcraft**
- **xbox**
- **xdcc**
- **yahoo**
- **yourfreetunnel**
- **zattoo**

- **pop3**
- **pptp**
- **rtcp**
- **rtp**
- **rtsp**
- **sdp**
- **secure-http**
- **sip**
- **smtp**
- **tcp**
- **tftp**
- **udp**
- **wsp**
- **wtp**

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear ACS analyzer statistics.

Example

The following command clears active charging service analyzer information for TCP analyzer:

```
clear active-charging analyzer statistics name tcp
```

clear active-charging charging-action statistics

Clears ACS charging action statistics.

Product

ACS

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear active-charging charging-action statistics [ name string ] [ | { grep grep_options
| more } ]
```

name *string*

Clears detailed information for an existing protocol analyzer.
string must be the name of an existing charging action.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear active charging action statistics.

Example

The following command clears active charging action statistics information for charging action named **pre-paid**:

```
clear active-charging charging-action statistics name pre-paid
```

clear active-charging content-filtering server-group statistics

Clears content filtering statistics for all CF server groups or a named CF server group.

Product

CF

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear active-charging content-filtering server-group statistics [ name srvrgrp_name ] [ |
{ grep grep_options | more } ]
```

name *srvrgrp_name*

Clears statistics for an existing CF server group, expressed as an alphanumeric string of 1 through 15 characters.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear content filtering statistics for CF server groups.

Example

The following command clears category-based content filtering statistics information for Rulebase named *cf_rule1*:

```
clear active-charging content-filtering category statistics rulebase name
cf_rule1
```

clear active-charging credit-control statistics

Clears credit control statistics.

Product

ACS

Privilege

Security Administrator, Administrator, Operator

Syntax

clear active-charging credit-control statistics [group *grp_name* **| server { ip-address** *ip_address* **| name** *name* **}]**

---

clear active-charging credit-control statistics

Clears statistics for all credit control groups.

---

group *grp_name*

Clears statistics for the credit control group specified as an alphanumeric string of 1 through 63 characters.

---

server { ip-address *ip_address* **| name** *name*

Clears statistics for the credit control server specified as:

- **ip-address**: an IP address for the credit control group entered in IPv4 dotted-decimal or IPv6 colon-separated notation
- **name**: name of the credit control group server entered as an alphanumeric string of 1 through 127 characters.

Usage

Use this command to clear credit control statistics.

Example

The following command clears statistics information for credit control:

```
clear active-charging credit-control statistics
```

clear active-charging dns-learnt-ip-addresses

Clears DNS learnt IP address statistics for the DNS Snooping feature.

Product

ACS

Privilege

Security Administrator, Administrator, Operator

Syntax

clear active-charging dns-learnt-ip-addresses statistics sessmgr { all | instance *sessmgr_instance* **} [| { grep** *grep_options* **| more }]**

sessmgr { all | instance *sessmgr_instance* **}**

Clears statistics for all or the specified Session Manager (SessMgr) instance.

- **all**: Clears statistics for all SessMgr instances.
- **instance** *sessmgr_instance*: Clears statistics for the specified SessMgr instance.

  sessmgr_instance must be an integer from 1 through 65535.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear DNS learnt IP address statistics for the DNS Snooping feature.
On clearing the statistics using this command, only the entries-flushed, entries-replaced, and IP-Overflows statistics are cleared as these are cumulative statistics. Total-entries will not be cleared as it is an instantaneous statistic of the current total entries in that rule line.

Example

The following command clears all DNS learnt IP address statistics:

```
clear active-charging dns-learnt-ip-addresses statistics sessmgr all
```

clear active-charging edr-format statistics

Clears ACS statistics for all Event Data Record (EDR) formats or a named EDR format.

Product

ACS

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear active-charging edr-format statistics [ name edr_format ]
```

name *edr_format*

Specifies name of the preconfigured EDR format for which you want to clear the statistics, expressed as an alphanumeric string of 1 through 63 characters.

Important: If an EDR format name is not specified, statistics for all EDR formats are cleared.

Usage

Use this command to clear the accumulated statistics for the specified EDR format.

Example

The following command clears the statistics for all EDR formats:

```
clear active-charging edr-format statistics
```

clear active-charging edr-udr-file statistics

Clears Event Data Record (EDR) and Usage Data Record (UDR) file related statistics.

Product

ACS

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear active-charging edr-udr-file statistics
```

Usage

Use this command to clear EDR and UDR file statistics.

Example

The following command clears statistical information for EDR and UDR files:

```
clear active-charging edr-udr-file statistics
```

clear active-charging firewall statistics

Clears Stateful Firewall statistics.

Product

FW

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear active-charging firewall statistics [ callid call_id | domain-name domain_name |
nat-realm nat_realm | protocol { icmp | icmpv6 | ip | ipv6 | other | tcp | udp } |
username user_name ] [ acsmgr instance instance_id ] [ | { grep grep_options | more } ]
```

acsmgr instance *instance_id*

Specifies an ACS Manager instance ID as an integer from 1 through 65535.

callid *call_id*

Specifies a call identification number as an eight-byte hexadecimal number.

domain-name *domain_name*

Specifies a domain name as an alphanumeric string of 1 through 127 characters.

nat-realm *nat_realm*

Specifies a NAT realm name as an alphanumeric string of 1 through 31 characters.

protocol { icmp | ip | other | tcp | udp }

Specifies a protocol for the statistics.

- **icmp**: ICMPv4
- **icmpv6**
- **ip**: IPv4
- **ipv6**
- **other**: Protocols other than TCP, UDP, and ICMPv4/ICMPv6
- **tcp**
- **udp**

username *user_name*

Specifies a user name as an alphanumeric string of 1 through 127 characters.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear Stateful Firewall statistics.

Example

The following command clears all Stateful Firewall statistics:

```
clear active-charging firewall statistics
```

clear active-charging firewall track-list

Clears the list of servers being tracked for involvement in any Denial-of-Service (DOS) attacks.

Product

FW

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear active-charging firewall track-list attacking-servers
```

Usage

Use this command to clear the list of servers being tracked for involvement in any DOS attacks.

Example

The following command clears the list of servers being tracked for involvement in any DOS attacks:

```
clear active-charging firewall track-list attacking-servers
```

clear active-charging fw-and-nat policy statistics

Clears statistics for all or a specific Firewall-and-NAT policy.

Product

FW, NAT

Privilege

Security Administrator, Administrator, Operator

Syntax

clear active-charging fw-and-nat policy statistics { all | name *policy_name* **} [| { grep** *grep_options* **| more }]**

all

Clears information for all configured firewall-and-NAT policies.

name *policy_name*

Clears information for the specified firewall-and-NAT policy, expressed as expressed as an alphanumeric string of 1 through 63 characters.

grep *grep_options***| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear statistics for all or a specific firewall-and-NAT policy.

Example

The following command clears statistics for the firewall-and-NAT policy named *test123*:

```
clear active-charging fw-and-nat policy statistics name test123
```

clear active-charging group-of-ruledefs statistics

Clears ACS group of ruledefs statistics.

Product

ACS

Privilege

Security Administrator, Administrator, Operator

Syntax

clear active-charging group-of-ruledefs statistics [name *group_of_ruledefs* **] [| { grep** *grep_options* **| more }]**

name *group_of_ruledefs*

Specifies the name of the group of ruledefs for which statistics must be cleared. *group_of_ruledefs* must be the name of an existing group of ruledefs expressed as an alphanumeric string of 1 through 63 characters.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear statistical information related to all or specified Active Charging Service group of ruledefs.

Example

The following command clears statistical information related to the group of ruledefs named *ruledef_group12*:

```
clear active-charging group-of-ruledefs statistics name ruledef_group12
```

clear active-charging nat statistics

Clears NAT realm statistics.

Product

NAT

Privilege

Security Administrator, Administrator, Operator

Syntax

clear active-charging nat statistics [nat-realm *nat_realm* **] [| { grep** *grep_options* **| more }]**

clear active-charging nat statistics

This command when issued in the local context clears statistics for all NAT realms in all contexts. When issued in a specific context, this command clears statistics for all NAT realms in that context.

clear active-charging nat statistics nat-realm *nat_realm*

This command when issued in the local context clears statistics for the specified NAT realm in all contexts. When issued in a specific context, this command clears statistics for the specified NAT realm in that context.

nat-realm *nat_realm*

Specifies name of the NAT realm as an alphanumeric string of 1 through 31 characters.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear NAT realm statistics.

Example

The following command when issued in the local context, clears NAT realm statistics for NAT realms named *test135* in all contexts:

```
clear active-charging nat statistics nat-realm test135
```

clear active-charging rulebase statistics

Clears ACS rulebase statistics.

Product

ACS

Privilege

Security Administrator, Administrator, Operator

Syntax

clear active-charging rulebase statistics [name *rulebase_name* **] [| { grep** *grep_options* **| more }]**

rulebase_name

Clears statistics for an existing ACS rulebase expressed as an alphanumeric string of 1 through 15 characters.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear ACS rulebase statistics.

Example

The following command clears statistics for the ACS rulebase named *postpaid*:

```
clear active-charging rulebase statistics name postpaid
```

clear active-charging ruledef statistics

Clears statistics for rule definitions configured in the Active Charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear active-charging ruledef statistics [ charging | firewall | name ruledef_name | tpo
] [ | { grep grep_options | more } ]
```

charging

Clears statistics for all configured Charging ruledefs.

firewall

Clears statistics for all configured Stateful Firewall ruledefs.

name *ruledef_name*

Clears statistics for the specified ruledef.
ruledef_name must be the name of an existing ruledef expressed as an alphanumeric string of 1 through 63 characters.

tpo

Important: The **tpo** keyword is available only in 12.2 and later releases.

Clears statistics for all configured Traffic Performance Optimization (TPO) ruledefs.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear ACS ruledef statistics.

Example

The following command clears all ruledef statistics:

```
clear active-charging ruledef statistics
```

clear active-charging subsystem

Clears all ACS subsystem information.

Product

ACS

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear active-charging subsystem
```

Usage

Use this command to clear all ACS subsystem information.

Example

The following command clears all ACS subsystem information:

```
clear active-charging subsystem
```

clear active-charging tcp-proxy statistics

Clears ACS TCP Proxy statistics.

Product

ACS

Privilege

Security Administrator, Administrator, Operator

Syntax

clear active-charging tcp-proxy statistics [all | ip-layer | proxy-fac | rulebase *rulebase_name* **| socket-migration | tcp-layer]**

all

Clears all TCP Proxy statistics.

ip-layer

Clears TCP Proxy statistics for IP layer.

proxy-fac

Clears TCP Proxy Flow Admission Control statistics.

rulebase *rulebase_name*

Clears TCP Proxy statistics for the rulebase specified as an alphanumeric string of 1 through 63 characters.

socket-migration

Clears TCP Proxy Socket Migration related statistics.

tcp-layer

Clears TCP Proxy statistics for TCP layer.

Usage

Use this command to clear TCP Proxy statistics.

Example

The following command clears TCP Proxy statistics for the rulebase named *test14*:

```
clear active-charging tcp-proxy statistics rulebase test14
```

clear active-charging tethering-detection statistics

Clears statistics pertaining to the Tethering Detection feature.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
clear active-charging tethering-detection statistics
```

Usage

Use this command to clear statistics pertaining to the Tethering Detection feature.

clear active-charging tpo policy statistics

Clears Traffic Performance Optimization (TPO) policy statistics.

Product

TPO

Privilege

Security Administrator, Administrator, Operator

Syntax

clear active-charging tpo policy statistics [name *tpo_policy_name* **]**

name *tpo_policy_name*

Clears statistics for an existing TPO policy specified as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to clear TPO policy statistics.

- **clear active-charging tpo policy statistics** command clears statistics for all TPO policies configured in the active charging service.
- **clear active-charging tpo policy statistics name** *tpo_policy_name* command clears statistics for the specified TPO policy.

Example

The following command clears statistics for the TPO policy named *policy12*:

```
clear active-charging tpo policy statistics name policy12
```

clear active-charging tpo profile statistics

Clears Traffic Performance Optimization (TPO) profile statistics.

Product

TPO

Privilege

Security Administrator, Administrator, Operator

Syntax

clear active-charging tpo profile statistics [name *tpo_profile_name* **]**

name *tpo_profile_name*

Clears statistics for an existing TPO profile specified as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to clear TPO profile statistics.

- **clear active-charging tpo profile statistics** command clears statistics for all TPO profiles configured in the active charging service.
- **clear active-charging tpo profile statistics name** *tpo_profile_name* command clears statistics for the specified TPO profile.

Example

The following command clears statistics for the TPO profile named *profile12*:

```
clear active-charging tpo profile statistics name profile12
```

clear active-charging url-blacklisting statistics

Clears URL Blacklisting feature related statistics.

Product

CF

Privilege

Security Administrator, Administrator, Operator

Syntax

clear active-charging url-blacklisting statistics [rulebase name *rulebase_name* **] [| { grep** *grep_options* **| more }]**

rulebase name *rulebase_name*

Clears URL Blacklisting information for an existing rulebase specified as an alphanumeric string of 1 through 63 characters.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear URL Blacklisting feature related statistics, optionally for a specific rulebase.

Example

The following command clears URL Blacklisting feature related statistics for *rulebase12*:

```
clear active-charging url-blacklisting statistics rulebase name
rulebase12
```

clear active-charging video detailed-statistics

Resets the detailed statistics for TCP video flows.

Product

MVG

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear active-charging video detailed-statistics
```

Usage

Use this command to reset the detailed statistics for TCP video flows.

Example

The following command resets the detailed statistics for TCP video flows:

```
clear active-charging video detailed-statistics
```

clear administrator

Ends the session of an administrative user specified by either user name or session ID.

Product

All

Privilege

Security Administrator, Administrator

Syntax

clear administrator { name *user_name* **| session id** *id_num* **}**

name *user_name*

Identifies the user name of the administrative user.

session id *id_num*

Identifies the ID number of the administrative user session as displayed in the output of the **show administrators session id** command.

Usage

This command is used to terminate command line interface sessions for other administrative users.

Example

The following command ends the session of the administrative user identified as *user1*:

```
clear administrator name user1
```

The following command ends the session of the administrative user with the session ID of *3*:

```
clear administrator session id 3
```

clear alarm

Clears outstanding alarm conditions

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

clear alarm { all | chassis | id *num* **| port** *slot/port* **| slot** *slot* **}**

all

Clear all outstanding alarms

chassis

Clears chassis-wide and fan tray alarms

id *num*

Clears a specific alarm by its internal alarm ID. *num* is the internal alarm identification number.

port *slot/port*

Clears alarms for the specified port. *slot/port* is the card slot and port on the card for which to clear alarms.

slot *slot*

Clears alarms for the specified slot. *slot* is the card slot for which to clear alarms.

Usage

Use this command to clear outstanding alarm conditions.

Example

To clear all outstanding alarms, use the following command:

```
clear alarm all
```

To clear all alarms for slot 7, enter the following command:

```
clear alarm slot 7
```

clear alcap

Clears the Access Link Control Application Part (ALCAP) session statistics of an ALCAP service associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

Product

HNB-GW

Privilege

Operator

Syntax

clear alcap statistics [alcap-service *alcap_svc_name* **[aal2-node** *aal2_node_name* **[aal2-path** *aal2_path_id* **]]]**

alcap-service *alcap_svc_name*

Specifies the name of the ALCAP service for which statistics are to be cleared.

aal2-node *aal2-node*

Specifies the name of the ATM Adaptation Layer 2 (AAL2) node for which ALCAP service statistics will be cleared.

aal2-path *aal2_path_id*

Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node for which ALCAP service statistics will be cleared.

Usage

This command is used to clear the sessions statistics and counters for ALCAP service.

Example

The following command clears the service session statistics of ALCAP service named as *alcap_hnb_svc1*:

```
clear alcap statistics alcap-service alcap_hnb_svc1
```

clear asngw-service

Clears the service session statistics for an Access Service Network Gateway (ASN-GW) service specified by either service name or trusted peer address.

Product

ANS-GW

Privilege

Security Administrator, Administrator

Syntax

clear asngw-service statistics [name *svc_name* **| peer-address** *ip_address* **]**

name *svc_name*

Identifies the name of the ASN-GW service for which statistics will be cleared. *svc_name* must be an alphanumeric string of 1 through 63 characters.

peer-address *ip_address*

Identifies the IP address of the ASN-GW peer for which service statistics will be cleared. *ip_address* must be entered in IPv4 dotted-decimal notation.

Usage

This command is used to terminate command line interface sessions for ASN GW services.

Example

The following command clears the service session statistics of the ASN-GW service named *aasn_svc1*:

```
clear asngw-service statistics name asn_svc1
```

clear asnpc-service

Clears the service session statistics of an ASN paging controller service specified by either ASN PC service name or trusted paging controller peer address.

Product

ANS-GW

Privilege

Security Administrator, Administrator

Syntax

clear asnpc-service statistics [name *svc_name* **| peer-address** *ip_address* **]**

name *svc_name*

Identifies the name of the ASN PC service for which session statistics will be cleared. *svc_name* must be an alphanumeric string of 1 through 63 characters.

peer-address *ip_address*

Identifies the IP address of the ASN PC peer for which all service statistics will be cleared. *ip_address* must be entered in IPv4 dotted-decimal notation.

Usage

This command is used to terminate command line interface sessions for ASN PC services.

Example

The following command clears the service session statistics of ASN PC service named as *asnpc_svc1*:

```
clear asnpc-service statistics name asnpc_svc1
```

clear apn statistics

Deletes all previously gathered statistics for either a specific Access Point Name (APN) or all APNs configured with the given context.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator, Operator

Syntax

clear apn statistics [name *apn_name* **| smgr-instance** *instance* **] [| { grep** *grep_options* **| more }]**

name *apn_name*

Specifies the name of a specific APN configured in the context for which to clear statistics. *apn_name* is the name of the APN expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

smgr-instance *instance*

Specifies a particular Sessmgr instance in the context for which to clear APN statistics. *instance* must be an integer from 1 to 4294967295.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Statistics for a single APN can be cleared using the **name** keyword. Statistics for all APNs in the context can be deleted by entering the command with no keywords.
If this command is executed from within the local context with no keywords, statistics will be cleared for every APN configured on the system regardless of context. In addition, if the **name** keyword is used when executing from within the local context, statistics for all APNs configured with the specified name will be cleared regardless of context.

Example

The following command clears statistics for an APN called *isp1*:

```
clear apn statistics name isp1
```

clear bcmcs statistics

Clears Broadcast Multicast Service (BCMCS) statistics.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear bcmcs statistics [pdsn-service *service_name* **]**

pdsn-service *service_name*

Specifies a specific PDSN service for which to clear BCMCS-specific statistics. This value must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to clear accumulated BCMCS statistics. You may specify an individual PDSN or peer to selectively clear statistics.

Example

```
clear bcmcs statistics

clear bcmcs statistics pdsn-service service_name
```

clear blacklisted-gtpu-bind-address

Clears the GTP-U loopback address blacklisted by a specific radio network controller (RNC) as defined for a specific IuPS Service configuration.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear blacklisted-gtpu-bind-address *ip_address* **rnc-id** *rnc_id* **mcc** *mcc_num* **mnc** *mnc_num* **iups-service** *name*

ip_address

Specifies the IP loopback address that has been blacklisted in IPv4 dotted-decimal notation. This loopback address was originally defined with the **associate-gtpu-bind-addfress** command in the Radio-Network-Controller Configuration mode of the IuPS Service.

Usage

This command enables this loopback address to be used for future RAB-assignment requests.

Example

```
clear blacklisted-gtpu-bind-address 1.1.1.1 rnc-id 2 mcc 123 mnc 321
iups-service iups1
```

clear bssap+ statistics

Clears the BSSAP+ protocol (base station subsystem GPRS protocol) statistics collected for the Gs interface between the SGSN and the MSC/VLR.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear bssap+ statistics [gs-service *gs_svc_name* **] [vlr { isdn-number** *ISDN_Num*| **name** *vlr_name* **}] [| { grep** *grep_options* **| more }]**

gs-service *gs_svc_name*

Specifies the name of a preconfigured Gs service handling BSSAP+ information as an alphanumeric string of 1 through 63 characters that is case sensitive.

vlr { isdn-number *ISDN_Num*| **name** *vlr_name*

Specifies a VLR (by ISDN number or name) handling BSSAP+ information.
isdn-number *ISDN_num* is the configured E.164-type ISDN number for the VLR. Enter a numerical string of 1 to 15 digits.
name *vlr_name* is the configured name of the VLR entered as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to delete or clear collected BSSAP+ protocol statistics for the entire SGSN or for a specified Gs interface. Using the keywords of this command, the interface can be identified by defining a specific VLR connected to the SGSN or by identifying the Gs service to which the interface has been configured.

Example

The following command clears the BSSAP+ statistics collected for the Gs interface configured for the Gs service named *gssvc1*.

```
clear bssap+ statistics gs-service gssvc1
```

clear bssgp statistics

Clears collected BSSGP protocol (base station subsystem GPRS protocol) statistics for traffic between the base station subsystem (BSS) and the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear bssgp statistics [gprs-service *gprs_svc_name* **| nse** *nse_id* **[bvc** *bvc_id* **] [| { grep** *grep_options* **| more }]**

gprs-service *gprs_svc_name*

Specifies the name of a preconfigured GPRS service for which the BSSGP statistics have been collected as an alphanumeric string of 1 through 63 characters that is case sensitive.

nse *nse_ID*

Clears the BSSGP statistics collected for the network service entity (NSE) specified as an integer from 0 through 65535.

bvc *bvc_ID*

Enter this keyword to clear the BSSGP statistics collected for the identified BSSGP virtual connection (BVC) specified as n integer from 0 through 65000.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear the BBSGP statistics for a particular GPRS service or NSEI.

Example

The following command deletes the collected BSSGP statistics for the GPRS service named *gprs1*.

```
clear bssgp statistics gprs-service gprs1
```

clear bulkstats

Clears counters and accumulated bulk statistics related information.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear bulkstats { counters | data }
```

counters

Clears the counters maintained by the system's "bulkstats" facility.

data

Clears any accumulated data that has not been transferred. This includes any "completed" files that have not been successfully transferred.

Usage

Once bulk statistics collection is enabled, the system stores the information until the specified transfer criteria is met or until a manual transfer is initiated. The system maintains counters for the "bulkstats" software facility. (Refer to the **data** keyword for the **show bulkstats** command for information on viewing the counters.)
This command can be used to delete bulk statistics information that has been collected but not transferred and/or to clear the counters that have been maintained.

Example

The following command clears bulk statistics-related counters:

```
clear bulkstats counters
```

clear cae-group statistics server

This command resets the discardable statistics, which are the Hit Count, Timeout Consecutive (Cumulative), and Last Failure statistics, for all CAEs or for a specific CAE. The CAE (Content Adaptation Engine) is an optional component of the Mobile Videoscape.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

clear cae-group statistics server { all | name *cae_name* **}**

all

Resets the discardable statistics for all CAEs.

name*cae_name*

Specifies the name of a CAE.

Usage

Use this command to reset the discardable statistics for all CAEs or for a specific CAE. This command must be issued in the same context in which the associated CAE group is defined.

Example

The following command clears the discardable statistics for the CAE named *server_1*:

```
clear cae-group statistics server name server_1
```

clear config

Replaces the active configuration source file with an empty configuration where possible.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
clear config [ -noconfirm ]
```

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

This command clears the current configuration when a complete overwrite is desired or if it is necessary to start from an empty configuration.

Important: Clearing the configuration will cause the active configuration source file to be empty and of no use in configuring the system to an active state providing service.

Important: This command should only be performed on configurations that have been previously backed up for easy restoration.

Example

The following command clears the active configuration after the user provides confirmation of the request.

```
clear config
```

The following command clears the active configuration source file immediately with no user confirmation.

```
clear config -noconfirm
```

clear congestion-control statistics

Clears the congestion control statistics for all instances of the specified manager type.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

clear congestion-control statistics {**a11mgr** | **asngwmgr** | **asnpcmgr** | **bindmux**|**hamgr** | **hnbmgr** | **gtpcmgr** | **ipsecmgr** | **imsimgr** | **l2tpmgr**}

a11mgr

Clears the statistics for all A11 Manager instances.

asngwmgr

Clears the statistics for all ASN GW Manager instances

asnpcmgr

Clears the statistics for all ASN PC-LR Manager instances

bindmux

Clears the statistics for all IPCF BindMux-Demux Manager instances.

hamgr

Clears the statistics for all HA Manager instances.

hnbmgr

Clears the statistics for all HNB Manager instances.

gtpcmgr

Clears the statistics for all GTPC Manager instances.

ipsecmgr

Clears the statistics for all IPSEC Manager instances.

imsimgr

Clears the statistics for all IMSI Manager instances.

l2tpmgr

Clears the statistics for all L2TP Manager instances.

Usage

Use this command to statistics for all instances of the specified manager.

Important: When this command is issued in any context other than the local context, only instances of the specified manager for the current context have the statistics cleared. When the current context is the local context, all instances of the specified manager type in all contexts have the statistics cleared.

Example

Clear the statistics for all instances of the A11 manger, by entering the following command:

```
clear congestion-control statistics a11mgr
```

clear content-filtering category statistics

Clears the Category-based Content Filtering application statistics.

Product

CF

Privilege

Security Administrator, Administrator, Operator

Syntax

clear content-filtering category statistics [facility srdbmgr instance *instance_value* **]**

facility srdbmgr instance *instance_value*

Clears logged events for the specified SRDB Manager instance.
instance_value must be an integer from 1 through 8.
In StarOS 9.0 and later releases, *instance_value* must be an integer from 1 through 10000.

Usage

Use this command to clear all Category-based Content Filtering application statistics, or statistics for a specific SRDB Manager instance.

Example

The following command clears all Category-based Content Filtering application statistics:

```
clear content-filtering category statistics
```

clear crash

Removes a specific crash file or all crash files.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

clear crash [list | number *crash_num* **]**

list | number *crash_num*

list: removes all crash files.
number *crash_num*: removes only the crash file specified as an integer from 1 through 30.

Usage

Clear crashes for general maintenance activities in cleaning out old, unused, or files which are of no importance.

Example

The following will remove all crash files.

```
clear crash list
```

The following command will remove only crash file *27*.

```
clear crash numer 27
```

clear credit-control statistics

Clears credit control statistics.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

clear credit-control statistics cc-service *cc_service_name*

cc-service *cc_service_name*

Specifies an existing Credit Control service name as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to clear active credit control statistics.

Example

The following command clears the configured credit control statistics for a service named *service1*:

```
clear credit-control statistics cc-service service1
```

clear crypto

Clears crypto associations or crypto statistics.

Product

PDSN, HA, GGSN, PDG/TTG, PDIF, SCM

Privilege

Security Administrator, Administrator, Operator

Syntax

clear crypto { isakmp [tag *map_name* **| peer** *peer_ip* **] | security-association { counters tag** *map_name* **[tx | rx] | tag** *map_name* **| peer** *peer_ip* **} | statistics { ikev2 | ipsec-3gpp-cscf | srtp } [service-ip-address** *ip-address* **| service-name** *name* **] }**

isakmp [tag *map_name* **| peer** *peer_ip* **]**

When no keywords are specified, this command clears all of the ISAKMP security associations for the current context.
tag *map_name*: Clears the ISAKMP SAs for the specified crypto map. *map_name* is the name of an existing crypto map.
peer *peer_ip*: Deletes the ISAKMP SAs for the specified peer. *peer_ip* must be entered in IPv4 dotted-decimal or IPv6 colon-separated notation.

security-association { counters map *map_name* **[tx | rx] | tag** *map_name* **| peer** *peer_ip* **}**

counters tag *map_name* **[tx | rx]**: Resets the counters for the specified crypto map. *map_name* is the name of an existing crypto map. **tx** specifies that only the transmit SA counters are reset. **rx** specifies that only the receive SA counters are reset. If neither **tx** or **rx** are specified, both transmit and receive SA counters are reset.
tag *map_name*: Tears down a Security Association (SA) for the specified crypto map. *map_name* is the name of an existing crypto map.
peer *peer_ip*: Clears the SAs for all tunnels who have the peer at the specified IP address. *peer_ip* must be entered in Pv4 dotted-decimal or IPv6 colon-separated notation.

Caution: Modification(s) to an existing crypto map and/or ISAKMP policy configuration will not take effect until the related security association has been cleared.

statistics { ikev2 | ipsec-3gpp-cscf | srtp } [service-ip-address *ip-address* **| service-name** *name* **]**

ikev2: Clears global IKEv2 statistics for the current context.
ipsec-3gpp-cscf: Clears global CSCF IPSec statistics for the current context.
srtp: Clears global CSCF SRTP (Secure Real-time Transport Protocol) statistics for the current context.
service-ip-address *ip-address*: Clears statistics for the specified service-ip address. **service-name** *name*: Clears statistics for the specified service name.

Usage

Clear SAs and apply changes to the crypto map or clear the crypto statistics for this context.

Example

The following clears all IKEv2 crypto statistics for the current context:

```
clear crypto statistics ikev2
```

clear cs-network statistics

Clears the HNB-Circuit Switched (CS) network service associated for an HNB-GW service instance.

Product

HNB-GW

Privilege

Operator

Syntax

clear cs-network statistics [name *cs_svc_name* **| ranap-only | rtp-only | sccp-only]**

name *cs_svc_name*

Clears the session statistics for an HNB-CS Network service name configured and running on this system. *cs_svc_name* must be an alphanumeric string of 1 through 63 characters.

ranap-only

Clears the session statistics limited to Radio Access Network Application Protocol (RANAP) traffic only for the specified HNB-CS Network service.

rtp-only

Clears the session statistics limited to Real Time Protocol (RTP) traffic only for the specified HNB-CS Network service.

sccp-only

Clears the session statistics limited to Signaling Connection Control Part (SCCP) traffic only for the specified HNB-CS Network service.

Usage

Use this command to clear the session statistics for overall session or in selected part of user session for HNB-CS Network services configured and running on a system.

Example

The following command clears the session statistics for RANAP part of session for the HNB-CS Network service *hnb_CS_1*:

```
clear cs-network statistics name hnb_CS_1 ranap-only
```

clear cscf service

Resets statistics counters for a specific Call/Session Control Function (CSCF) service, all CSCF services, or for all services within a specified context (VPN).

Product

SCM

Privilege

Security Administrator, Administrator, Operator

Syntax

clear cscf service { diameter { location-info | policy-control } statistics [service-name *service_name* **| vpn-name** *name* **] | li-packet-cable statistics [service-name** *service_name*] **| performance-counters name** *service_name* **| statistics name** *service_name* **{ all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp { msrp | sip } | vpn-name** *name* **{ all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp { msrp | sip } } }**

---

diameter { location-info | policy-control } statistics [service-name *service_name* **| vpn-name** *name* **]**

Clears Diameter (DPECA) statistics on the CSCF Rx interface with the configuration information.
service-name *service_name*: Specifies the name of an existing CSCF service for which the statistics will be reset as an alphanumeric string of 1 through 63 characters.
vpn-name *name*: Specifies the name of an existing context in which all statistics for all services will be reset as an alphanumeric string of 1 through 79 characters.

---

li-packet-cable statistics [service-name *service_name* **]**

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

---

performance-counters name *service_name*

Clears all CSCF performance counters for an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.

---

statistics name *service_name* **{ all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp tcp { msrp | sip } | vpn-name** *name* **{ all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp tcp { msrp | sip } } }**

Clears service statistics for an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.
all: Clears all CSCF service statistics.
calls: Clears statistics related to CSCF calls.
ip-security: Clears statistics related to CSCF IPSec.
message: Clears statistics for the SIP method MESSAGE.
package-name: Clears statistics for the associated event package.

- **message-summary**: Clears statistics for the “message-summary” event package.
- **presence**: Clears statistics for the “presence” event package.

- **reg**: Clears statistics for the “reg” event package.
- **winfo**: Clears statistics for the “watcher-info” event package.

registrations: Clears statistics related to CSCF registrations, re-registrations, and de-registrations.
sigcomp: Clears statistics related to CSCF sigcomp.
tcp: Displays session statistics related to CSCF TCP.

- **msrp**: Clears statistics related to CSCF MSRP TCP.
- **sip**: Clears statistics related to CSCF SIP TCP.

vpn-name *name*: Clears statistics for a specific CSCF service configured in a specific context on this system. *name* must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

Important: This keyword must be followed by another statistics-related keyword.

Usage

Use this command to reset statistics counters for CSCF services. This command will reset the counters in the output of the **show cscf service statistics** command.

Important: This command will not clear current registered users and current CSCF sessions.

Example

The following command resets all statistics for a service named *cscf1*:

```
clear cscf service statistics name cscf1 all
```

clear cscf sessions

Clears statistics for Call/Session Control Function (CSCF) sessions on this system.

Product

SCM

Privilege

Security Administrator, Administrator, Operator

Syntax

clear cscf sessions { counters { calls | subscription } service *service_name* **| service** *service_name* **{ all | aor** *aor* **| session-id** *id* **}**

---

counters { calls | subscription } service *service_name*

Clears counters for all CSCF sessions matching the filter criteria.
calls: Counters associated with calls in CSCF service.
subscription: Counters associated with subscriptions in CSCF service.
service *service_name*: Counters on specific CSCF service. *service_name* must be an existing CSCF service expressed as an alphanumeric string of 1 through 63 alphanumeric characters.

---

service *service_name* **{ all | aor** *aor* **| session-id** *id* **}**

Clears session information for all CSCF sessions matching the filter criteria.
service *service_name*: Session statistics on specific CSCF service. *service_name* must be an existing CSCF service expressed as an alphanumeric string of 1 through 63 alphanumeric characters.

- **all**: Specifies that session statistics are to be cleared for all sessions on this service.
- **aor** *aor*: Specifies that session statistics are to be cleared for sessions at this specific AoR. *aor* must be an existing AoR expressed as an alphanumeric string of 1 through 79 characters.
- **session-id** *id*: Specifies that session statistics are to be cleared for sessions with this ID. *id* must be an existing session ID expressed as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to clear session information for CSCF sessions.

Example

The following command resets all session statistics for a service named *cscf1*:

```
clear cscf sessions service cscf1 all
```

clear cscf sip

Resets SIP statistics counters for a specific CSCF service, all CSCF services, or for all services within a specified context (VPN) or interface.

Product

SCM

Privilege

Security Administrator, Administrator, Operator

Syntax

clear cscf sip statistics [name *service_name* **[interface { domain name** *domain_name* **| ip address** *ip_address* **} | vpn-name** *name* **]**

name *service_name*

Specifies the name of an existing CSCF service for which the SIP statistics will be reset as an alphanumeric string of 1 through 63 characters.

interface { domain name *domain_name* **| ip address** *ip_address* **}**

SIP statistics will be reset in this interface.
domain name *domain_name*: Specifies an existing domain associated with the CSCF service as an alphanumeric string of 1 through 64 characters.
ip address *ip_address*: Specifies the destination or source ip address associated with the CSCF service.

vpn-name *name*

Specifies the name of an existing context in which all SIP statistics for all services will be reset as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to reset SIP counters found in the output of the **show cscf sip** command.

Example

The following command resets the SIP statistics for a service named *cscf1*:

```
clear cscf sip statistics name cscf1
```

clear cscf subscription

Clears all subscriptions for a named service or for individual subscribers within the service.

Product

SCM

Privilege

Security Administrator, Administrator, Operator

Syntax

clear cscf subscription service *service_name* **{ all | from-aor** *subscriber_aor* **to-aor** *resource_aor* **}**

service *service_name*

Specifies the name of an existing CSCF service for which the subscription(s) will be cleared as an alphanumeric string of 1 through 63 characters.

all | from-aor *subscriber_aor* **to-aor** *resource_aor*

all: Removes all CSCF subscriptions for the specified service.
from-aor *subscriber_aor*: Removes all CSCF subscriptions for a specified subscriber in a specified service.
subscribed-to *resource_aor*: Removes all CSCF subscriptions for a specified subscriber in a specified service with a specified subscribed-to resource AoR.

Usage

Use this command to clear subscriptions to enforce policies. This command initiates a SUBSCRIBE request with Expires as 0 in the corresponding subscription dialog.

Example

The following command clear all subscriptions for a CSCF service named *cscf1*:

```
clear cscf subscription service cscf1 all
```

clear diameter-service

Clears information pertaining to configured Diameter services.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

clear diameter-service { eap { all | session-id *session_id* **} | lte-s6b { all | session-id** *session_id* **} | lte-sta { all | session-id** *session_id* **} | mbms { bearer-contexts { all | bmsc-bearer-service name** *service_name* **} | ue-context { all | bmsc-bearer-service name** *service_name* **} } | statistics name** *service_name* **[vpn-name** *vpn context_name* **] }**

---

eap { all | session-id *session_id* **}**

Clears subscribers from the EAP interface.
all: Clears all subscribers.
session-id *session_id*: Clears a call for the session ID specified as an alphanumeric string of 1 through 63 characters.

---

lte-s6b { all | session-id *session_id* **}**

Clears subscribers from the S6b interface.
all: Clears all subscribers.
session-id *session_id*: Clears a call for the session ID specified as an alphanumeric string of 1 through 63 characters.

---

lte-sta { all | session-id *session_id* **}**

Clears subscribers from STa interface.
all: Clears all subscribers.
session-id *session_id*: Clears a call for the session ID specified as an alphanumeric string of 1 through 63 characters.

---

mbms { bearer-contexts { all | bmsc-bearer-service name *service_name* **} | ue-context { all | bmsc-bearer-service name** *service_name* **} }**

Clears information from the SGSN-APP interface.
bearer-contexts { all | bmsc-bearer-service name *service_name* **}**: Clears information from the bearer-context gmb-interface.
all: Clears all subscribers.
bmsc-bearer-service name *service_name* **}**: Specifies the name of a bmsc-bearer-service as an alphanumeric string of 1 through 63 characters.
ue-context { all | bmsc-bearer-service name *service_name* **}**: Clear information UE context for gmb-interface.
all: Clears all subscribers.
bmsc-bearer-service name *service_name* **}**: Specifies the name of a bmsc-bearer-service as an alphanumeric string of 1 through 63 characters.

service_name

service_name must be a name of a Diameter service expressed as an alphanumeric string of 1 through 63 characters.

statistics name *service_name* **[vpn-name** *vpn context_name* **]**

Clears the Diameter service associated with the specified statistics.
name *service_name*: Specifies the name of a Diameter service as an alphanumeric string of 1 through 63 characters.
vpn-name *vpn context_name*: Clears statistics for the vpn-context name specified as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to clear information pertaining to configured Diameter services.

Example

The following command clears Diameter service information for all subscribers associated with EAP interface:

```
clear diameter-service eap all
```

clear diameter aaa-statistics

Clears Diameter AAA statistics.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

clear diameter aaa-statistics [all | [group *aaa_group* **] server** *diameter_server* **] [| { grep** *grep_options* **| more }]**

all

Clears all Diameter server statistics.

group *aaa_group*

Clears Diameter server statistics for the AAA group specified as an alphanumeric string of 1 through 64 characters.

server *diameter_server*

Clears Diameter server statistics for the Diameter server specified as an alphanumeric string of 1 through 64 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear Diameter AAA statistics.

Example

The following command clears Diameter server statistics for the specified AAA group:

```
clear diameter aaa-statistics group aaagroup3
```

clear diameter statistics

Clears Diameter statistics.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

clear diameter statistics [[proxy] endpoint *endpoint_name* **[peer-host** *host_id* **[peer-realm** *realm_id* **]]] [| { grep** *grep_options* **| more }]**

endpoint *endpoint_name*

Clears endpoint-related statistics for the endpoint expressed as an alphanumeric string of 1 through 63 character.

proxy

Clears proxy related statistics.

peer-host *host_id*

Clears statistics for the Diameter peer host ID specified as an alphanumeric string of 1 through 255 characters.

peer-realm *realm_id*

Clears statistics for the Diameter peer realm specified as an alphanumeric string of 1 through 127 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear Diameter statistics.

Example

The following command clears all Diameter statistics for the specified endpoint:

```
clear diameter statistics endpoint endpt345
```

clear dhcp statistics

Deletes all previously gathered statistics for either a specific DHCP server or all DHCP servers configured within the given context.

Product

GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear dhcp statistics [ dhcp-service svc_name | server ip_address ]
```

dhcp-service *svc_name*

Specifies the name of a specific DHCP service for which to clear statistics as an alphanumeric string of 1 through 63 characters that is case sensitive.

server *ip_address*

Specifies the IP address of a DHCP server in IPv4 dotted-decimal notation as configured in the context for which to clear statistics.

Usage

Statistics for a single server can be cleared using the **server** keyword. Statistics for all DHCP servers in the context can be deleted by entering the command with no keywords.
This command can be executed from any context configured on the system.
If this command is executed from within the local context with no keywords, statistics will be cleared for every DHCP server configured on the system regardless of context. In addition, if the server keyword is used when executing from within the local context, statistics for all DHCP servers configured with the specified name will be cleared regardless of context.

Example

The following command clears statistics for all configured DHCP servers within the context:

```
clear dhcp statistics
```

clear dns-client

Clears DNS cache and/or statistics for a specified DNS client.

Product

SCM

Privilege

Security Administrator, Administrator, Operator

Syntax

clear dns-client *name* **{ cache [query-name** *name* **| query-type { A | AAAA | NAPTR | SRV }] | statistics }**

dns-client *name*

Specifies the name of an existing DNS client whose cache and/or statistics are being cleared as an alphanumeric string of 1 through 255 characters.

cache [query-name *name* **| query-type { A | AAAA | NAPTR | SRV }]**

Specifies that the cache for the defined DNS client is to be cleared.
query-name *name*: Filters DNS results based on the domain name. The name is an alphanumeric string of 1 through 255 characters. that is the domain name used to perform the DNS query. This name is different from the actual domain name which is resolved. For example, to resolve the SIP server for *service.com*, the query name is *_sip._udp.service.com* and the query type is **SRV**.
query-type:

- **A**: Filters DNS results based on domain IP address records (A records).
- **AAAA**: Filters DNS results based on AAAA records (AAAA resource records).
- **NAPTR**: Filters DNS results based on Name Authority Pointer records.
- **SRV**: Filters DNS results based on service host records (SRV records).

statistics

Specifies that statistics for the defined DNS client are to be cleared.

Usage

Use this command to clear DNS cache and/or statistics for a specified DNS client.

Example

The following command clears statistics for a DNS client named *domain1.com*:

```
clear dns-client domain1.com statistics
```

clear egtpc

Clears enhanced GPRS Tunneling Protocol control plane (eGTP-C) statistics and counters found in **show** command outputs and bulk statistics associated with all eGTP-C-related services or those defined by the parameters in this command.

Product

MME, P-GW, S-GW

Privilege

Operator

Syntax

clear egtpc statistics [egtp-service *name* **| interface-type { interface-mme | interface-pgw-ingress | interface-sgw-egress | interface-sgw-ingress } | mme-address** *ip_address* **| pgw-address** *ip_address* **| sgw-address** *ip_address* **]**

---

egtp-service *name*

Clears all statistics and counters associated with an existing eGTP service name specified as an alphanumeric string of 1 through 63 characters.

---

interface-type { interface-mme | interface-pgw-ingress | interface-sgw-egress | interface-sgw-ingress }

interface-mme: Clears statistics and counters derived from all MME interface types associated with this system.
interface-pgw-ingress: Clears statistics and counters derived from all P-GW ingress interface types associated with this system.
interface-sgw-egress: Clears statistics and counters derived from all S-GW egress interface types associated with this system.
interface-sgsn: Clears statistics and counters derived from all SGSN S4 interface types associated with this system.
interface-sgw-ingress: Clears statistics and counters derived from all S-GW ingress interface types associated with this system.

---

mme-address *ip_address*

Clears all statistics and counters derived from an existing MME IP address specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

---

pgw-address *ip_address*

Clears all statistics and counters derived from an existing P-GW IP address specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

---

sgw-address *ip_address*

Clears all statistics and counters derived from an existing S-GW IP address specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

sgsn-address *ip_address*

Clears all statistics and counters derived from an existing SGSN S4 IP address specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to clear running statistics and counters found in show command and bulk statistics outputs for all eGTP-C-related services or for specific interfaces, services, or IP addresses as specified by parameters in this command.

Example

The following command clears eGTP-C statistics and counter associated with all P-GW ingress interfaces configured on this system:

```
clear egtpc statistics interface-type interface-pgw-ingress
```

The following command clears eGTP-C statistics and counter associated with all MME interfaces configured on this system:

```
clear egtpc statistics interface-type interface-mme
```

clear event-notif statistics

Clears the statistical information collected over a configured Event Notification (SNMP) interface based on specific criteria.

Product

All

Privilege

Inspector

Syntax

```
clear event-notif statistics
```

Usage

Use this command to clear the statistical information collected over configured Event Notification interface based on specific criteria.

Example

The following command clears the counter information for all Event Notification collection servers configured in a context:

```
clear event-notif server all
```

clear firewall

This command is obsolete.

clear fng-service statistics

Deletes all previously gathered statistics for a specific Femto Network Gateway (FNG) service or all FNG services configured within a context.

Product

FNG

Privilege

Security Administrator, Administrator, Operator

Syntax

clear fng-service statistics {name *service_name***}**

name *service_name*

Specifies the name of a specific FNG service configured in the context for which to clear statistics as an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage

Statistics for a single FNG service can be cleared using the **name** keyword. Statistics for all FNG services in the context can be deleted by entering the command with no keywords.
If this command is executed from within the local context with no keywords, statistics will be cleared for every FNG service configured on the system regardless of context. In addition, if the **name** keyword is used when executing from within the local context, statistics for all FNG services configured with the specified name will be cleared regardless of context.

Example

The following command clears statistics for an FNG service named fng1:

```
clear fng-service statistics name fng1
```

clear gmm-sm statistics

Deletes the collected statistics for the GPRS Mobility Management and Session Management (GMM/SM) configurations for various SGSN services.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

clear gmm-sm statistics [gmm-only | plmn-id mcc *mcc* **mnc** *mnc* **[access-type { gprs | umts }] | sm-only] [gprs-service** *srvc_name* **| iups-service** *srvc_name* **| sgsn-service** *srvc_name* **]**

Keywords are presented below. First are the primary keywords in the order one is selected, as displayed in the syntax. Secondary or filtering keywords are presented alphabetically after the primary keywords.

gmm-only

Deletes only GPRS mobility management (GMM) information for the specified keyword parameters.

plmn-id mcc *mcc* **mnc***mnc* **[access-type { gprs | umts }]**

Deletes the statistics for services within a specified PLMN.
Enter the **access-type** keyword to fine-tune the delete procedure and only delete GMM/SM statistics for the IuPS (select access-type UMTS) and/or the GPRS (select access-type GPRS) services belonging to the PLMN.

sm-only

Deletes only session management (SM) information for the specified keyword parameters.

gprs-service *srvc_name*

Deletes the statistics for a 2.5G GPRS service specified as an alphanumeric string of 1 through 63 characters that uniquely identifies a preconfigured GPRS service. The delete request can be narrowed by adding either the **nsei** or **routing-area** keywords.

iups-service *srvc_name*

Deletes the statistics for a IuPS service specified as an alphanumeric string of 1 through 63 characters that uniquely identifies a preconfigured IuPS service. The delete request can be narrowed by adding either the **rnc** or **routing-area** keywords.

sgsn-service *srvc_name*

Deletes the statistics for a 3G SGSN service specified as an alphanumeric string of 1 through 63 characters that uniquely identifies the SGSN service. The delete request can be narrowed by adding either the **rnc** or **routing-area** keywords.

access-type *type*

Defines the type of access to be allowed or restricted.

- **eps**
- **gprs**
- **umts**

If this keyword is not included, both access types are allowed by default.

lac *lac_id*

Specifies the location area code (LAC) as part of the identification of the RNC or RA. *lac_id* must be an integer from 1 through 65535.

mcc *mcc_id*

Specifies the mobile country code (MCC) as part of the identification of the RNC or RA. *mcc_id* must be an integer from 100 through 999.

mnc *mnc_id*

Specifies the mobile network code (MNC) as part of the identification of the RNC or RA. *mnc_id* must be a 2- or 3-digit integer from 00 through 999.

nsei*nse_id*

Deletes the GMM/SM session statistics for the identified network service entity (NSEI). *nse_id* must be an integer from 0 through 65535 that uniquely identifies a configured NSEI.

rnc*rnc_id*

Fine-tunes the deletion of GMM/SM session statistics just for the specified radio network controller (RNC). *rnc_id* must be an integer from 0 through 4095.

rac *rac_id*

Specifies the routing area code (RAC) as part of the identification of the RNC or RA. *rac_id* must be an integer from 1 through 255.

routing-area mcc *mcc_id* **mnc** *mnc_id* **lac** *lac_id* **rac** *rac_id*

Enter the **routing-area** keyword to fine-tune the clearing of the GMM/SM statistics for a specified routing area (RA) identified by the MCC, MNC, LAC and RAC.

Usage

Use this command to delete usage statistics for the GMM/SM session configurations for SGSN services, including a BSC's attaches, activations, and throughput.

Example

The following command deletes GMM/SM statistics for a specific routing area defined for the SGSN's GPRS service:

```
clear gmm-sm statistics gprs-service gprs1 routing-area mcc 123 mcc 131
lac 24 rac 11
```

The following command displays all possible information for GMM/SM statistics:

show gmm-sm statistics verbose

Important: Output descriptions for **show** commands are available in the *Statistics and Counters Reference*.

clear gprsns statistics

Deletes collected statistics for the 2.5G SGSN's General Packet Radio Service (GPRS) Network Service (NS) layer (link level).

Product

SGSN

Privilege

Inspector

Syntax

clear gprsns statistics { msg-stats nse *nse_id* **| sns-msg-stats }[| { grep** *grep_options* **| more }]**

msg-stats

Deletes collected transmit (tx) and receive (rx) message statistics for the NS layer.

consolidated nse *nse_id*

nse_id: Enter an integer from 0 to 65535.

nse *nse_id*

Deletes statistics for an NSE specified as an integer from 0 to 65535.

sns-msg-stats

Deletes subnetwork service (SNS) sublayer message statistics.

| { grep *grep_options* **| more }**

You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

This command is used to display Frame Relay statistics configured for the NSE/NSVC with the commands documented in the *Network Service Entity - Peer NSEI Configuration Mode* chapter.
Collected statistics are cleared (deleted) with the **clear gprsns statistics** described in the *Exec Mode Commands (A-C)* chapter.

Example

The following command displays the collected message statistics for NSEI *1422*:

```
show gprsns statistics msg-stats nse 1422
```

Important: Output descriptions for **show** commands are available in the *Statistics and Counters Reference*.

clear gprsssf statistics

Deletes all Customized Applications for Mobile networks Enhanced Logic (CAMEL) service gprsSSF statistics collected since the last reset or **clear** command.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear gprsssf statistics [camel-service *srvc_name* **| gprs [2g-sgsn-app | 3g-sgsn-app] | gsmscf-address {** *address* **| all } | sms] [| { grep | more }]**

camel-service *srvc_name*

Clears only CAMEL service statistics for the configured CAMEL service specified as an alphanumeric string of 1 through 63 characters.

gprs [2g-sgsn-app | 3g-sgsn-app]

Clears only CAMEL service statistics for either a 2.5G or 3G SGSN.

gsmscf-address { *address* **| all }**

Filters the command to only clear CAMEL service statistics for specified GSM service control function (gsmSCF) addresses. *address* is a standard ISDN E.164 address of 1 to 15 digits.

sms

Filters the command to only clear CAMEL service statistics for SMS protocol information.

| { grep *grep_options* **| more }**

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

This command instructs the SGSN to delete collected CAMEL service statistics for either specified CAMEL services, or for SMS or GPRS applications in all contexts.

Example

The following command will delete gprsSSF statistics collected for the CAMEL service residing at SCP identified by the gsmSCF address:

```
clear gprsssf statistics gsmscf-address 412211411151
```

clear gtpc statistics

Deletes all previously gathered GTPC (GTPv0, GTPv1-C, GTPv1-U) statistics within the given context based on the specified criteria.

Product

GGSN, MSEG

Privilege

Security Administrator, Administrator, Operator

Syntax

clear gtpc statistics [[custom1 | gtpcmgr-instance *gtpcmgr_instance_number* **| smgr-instance** *sessmgr_instance_number* **] [apn** *apn_name* **| ggsn-service** *ggsn_service_name* **| mseg-service** *mseg_service_name* **| sgsn-address** *sgsn_ipv4_address* **]]**

custom1

Clears the statistics of GTP-C messages for preservation mode and free of charge service.
This keyword is a customer-specific function used for Preservation-Mode and Free-of-Charge Service that is enabled under customer-specific license. For more information on this support, contact your Cisco account representative.

gtpcmgr-instance *gtpcmgr_instance_number*

Clears GTP-C statistics for a GTPC Manager instance specified as an integer from 1 through 4294967295.

smgr-instance *sessmgr_instance_number*

Clears GTP-C statistics for a Session Manager instance specified as an integer from 1 through 4294967295.

apn *apn_name*

Clears GTP-C statistics for an existing APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

ggsn-service *ggsn_service_name*

Clears GTP-C statistics for an existing GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

mseg-service *mseg_service_name*

Important: This keyword is not supported in this release. For more information please contact your Cisco account representative.

Clears GTP-C statistics for an existing MSEG service specified as an alphanumeric string of 1 through 63 characters.

sgsn-address *sgsn_ipv4_address*

Clears GTP-C statistics for an existing SGSN specified by IP address in IPv4 dotted-decimal notation.

Usage

GTPC statistics can be cleared for a single APN, GGSN service, or SGSN. All GTPC statistics in the context can be deleted by entering the command with no keywords.
This command can be executed from any context configured on the system.
If this command is executed from within the local context with no keywords, all GTPC statistics will be cleared regardless of context.
GTPP statistics are not affected by this command.

Example

The following command clears all GTPC statistics context:

```
clear gtpc statistics
```

clear gtpp statistics

Deletes all previously gathered GTPP statistics within the given context based for either single or all charging gateway functions (CGFs).

Product

GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear gtpp statistics [cgf-address *ip-address* **]**

cgf-address *cgf_address*

Deletes statistics for a CGF identified by its IP address entered in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Statistics for a single CGF can be cleared using the **cgf-address** keyword. Statistics for all CGFs in the context can be deleted by entering the command with no keywords.
This command can be executed from any context configured on the system.
If this command is executed from within the local context with no keywords, statistics will be cleared for every CGF configured on the system regardless of context. In addition, if the cgf-address keyword is used when executing from within the local context, statistics for all CGFs configured with the specified name will be cleared regardless of context.

Example

The following command deletes all GTPP statistics for a CGF with an IP address of 192.168.1.42:

```
clear gtpp statistics cgf-address 192.168.1.42
```

clear gtpp storage-server local file statistics

Clears AAA proxy GTPP group level statistics for CDRs stored on the local SMC hard disk.

Product

GGSN, SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear gtpp storage-server local file statistics [ group name name ]
```

Usage

If executed from the local context, this command clears statistics for all GTPP groups configured on the system. If executed from the context within which the storage servers (SMC hard disk) is configured, statistics are deleted for only that context.

clear gtpp storage-server statistics

Clears statistics for configured GTPP storage servers (GSS).

Product

GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear gtpp storage-server statistics
```

Usage

If executed from the local context, this command clears statistics for all GTPP storage servers configured on the system. If executed from the context within which the servers are configured, statistics are deleted for only those servers.

clear gtpu statistics

Clears enhanced GPRS Tunneling Protocol user plane statistics and counters found in **show** command outputs and bulk statistics associated with all GTP-U-related services or those defined by the parameters in this command.

Product

P-GW, S-GW, MSEG

Privilege

Operator

Syntax

clear gtpu statistics [gtpu-service *gtpu_service_name* **| mseg-service** *mseg_service_name* **| peer-address** *ipv4/ipv6_address* **]**

gtpu-service *gtpu_service_name*

Clears GTP-U statistics for an existing GTP-U service specified as an alphanumeric string of 1 through 63 characters.

mseg-service *mseg_service_name*

Important: This keyword is not supported in this release. For more information please contact your Cisco account representative.

Clears GTP-U statistics for an existing MSEG service specified as an alphanumeric string of 1 through 63 characters.

peer-address *ipv4/ipv6_address*

Clears GTP-U statistics for an existing peer IP address entered in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to clear running statistics and counters found in show command and bulk statistics outputs for all GTP-U-related services or for specific services or IP addresses as specified by parameters in this command.

Example

The following command clears GTP-U statistics and counter associated with a GTP-U service name *gtpu-12* configured on this system:

```
clear gtpu statistics gtpu-service gtpu-12
```

clear hd-storage-policy

Clears statistic information for HD storage policies configured on the system.

Product

HSGW, P-GW, S-GW

Privilege

Operator

Syntax

clear hd-storage-policy statistics { all | name *name* **}**

statistics { all | name *name* **}**

all: Clears ACR statistical information for all HD storage policies configured on the system.
name *name*: Clears ACR statistical information for an existing HD storage policy specified as an alphanumeric string of 0 through 63 characters.

Usage

Use this command to clear statistics for HD storage policies configured on the system.

Example

The following command clears statistics for an HD storage policy named *pgwsgw*:

```
clear hd-storage-policy statistics name pgwsgw
```

clear hnbgw sessions

Clears the active/dormant session information about registered Nabs) on Home-NodeB Gateway (HNB-GW) service instances configured and running on this system based on different filter criteria.

Product

HNB-GW

Privilege

Operator

Syntax

clear hnbgw sessions {**all** | **cell-id** *cell_id* | **hnb-address** *hnb_ip_address* | **hnb-local-id** *hnb_id* | **hnbgw-service** *hnbgw_svc_name* | **hnbid** *hnb_glbl_id* | **mcc** *mcc* **mnc** *mnc* [**noconfirm**] [**lac** *lac* | **rac** *rac*]}

all

Clears the summarized or full information for all registered HNB sessions on an HNB-GW service instance running on system. Clearing the statistics can be filtered based on given filtering.

cell-id *cell_id*

Clears HNB session statistics for a registered cell ID on an HNB-GW service instance. *cell_id* is the identification number of the Femto cell where the user/subscriber is geographically located expressed as an integer from 0 through 268435455.

hnb-address *hnb_ip_address*

Clears the session statistics for HNB session(s) based on a registered HNB IP address entered in IPv4 dotted-decimal notation.

hnb-local-id *hnb_id*

Clears the session statistics of HNB session(s) for a registered local id of HNB specified as as an integer from 1 through 255.

hnbgw-service *hnbgw_svc_name*

Clears the session statistics for registered HNB session(s) on an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

hnbid *hnb_glbl_id*

Clears the statistics for HNB session(s) based on the registered HNB global id specified as an integer from 1 through 255

mcc *mcc*

Clears statistics for HNB session(s) based on the registered Mobile Country Code (MCC) identification number of the UE. *mcc* must be an integer from 101 through 999.

mnc *mnc*

Clears the statistics for HNB session(s) based on the registered Mobile Network Code (MNC) identification number of the UE. *mnc* must be a 2- or 3-digit integer from 00 through 999

lac *lac*

Clears the statistics for HNB session(s) based on the registered Location Area Code (LAC) identification number of the UE. *lac* must be an integer from 1 through 65535.

rac *rac*

Clears the statistics for HNB session(s) based on the registered Radio Access Code (RAC) identification number of the UE. *rac* must be an integer from 1 through 255.

rnc *rnc*

Clears the statistics for HNB session(s) based on the registered Radio Network Code (RAC) identification number of the HNB. *rnc* must be an integer from 1 through 65535.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Important: The Operator privilege does not have access to this keyword.

Usage

Use this command to clear the session statistics of all or specific registered HNB session(s) or in selected part of user session for HNB-GW services configured and running on this system.

Example

The following command clears the session statistics for all registered HNBs on the HNB-GW service named *hnbgw1*:

```
clear hnbgw sessions hnbgw-service hnbgw1
```

clear hnbgw statistics

Clears the HNB-GW service and HNB related statistics from an HNB-GW node.

Product

HNB-GW

Privilege

Operator

Syntax

```
clear hnbgw statistics { hnbgw-service hnbgw_svc_name [ gtpu-only | hnbap-only | ranap-
only | rtp-only | rua -only | sccp-only | sctp-only ] | hnbid hnb_identifier [ gtpu-only
| hnbap-only | ranap-only | rtp-only | rua -only ] }
```

hnbgw-service *hnbgw_svc_name*

Clears the session statistics for an existing \HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

hnbid *hnb_identifier*

Clears the session statistics for an existing Home-NodeB identifier specified as an alphanumeric string of 1 through 255 characters.

gtpu-only

Clears the statistics for GTP-U traffic only for the selected HNB/HNB-GW service.

hnbap-only

Clears the statistics for Home NodeB Application Part (HNBAP) traffic only for the selected HNB/HNB-GW service.

ranap-only

Clears the session statistics for Radio Access Network Application Protocol (RANAP) traffic only for the selected HNB/HNB-GW service.

rtp-only

Clears the session statistics for Real Time Protocol (RTP) traffic only for the selected HNB/HNB-GW service.

rua-only

Clears the session statistics for RANAP User Adaptation (RUA) traffic only for the selected HNB/HNB-GW service.

sccp-only

Clears the session statistics for Signaling Connection Control Part (SCCP) traffic only for the selected HNB-GW service.

sctp-only

Filters the session statistics to display only Stream Control Transmission Protocol (SCTP) traffic for the selected HNB-GW service.

Usage

Use this command to clear the session statistics for an overall session or in a selected part of a user session for HNB-GW services and/or HNBs configured and running on this system.

Example

The following command clear the session statistics for the HNBAP portion of session details for the HNB-GW service named *hnbgw1*:

```
clear hnbgw statistics hnbgw-service hnbgw1 hnbap-only
```

The following command clears the session statistics for the RANAP portion of session details for the HNB identified as *102*:

```
clear hnbgw statistics hnbid 102 ranap-only
```

clear hsgw-service

Clears HRPD Serving Gateway (HSGW) statistics and counters found in **show** command outputs and bulk statistics associated with all HSGW services or a specific service defined by the parameter in this command.

Product

HSGW

Privilege

Operator

Syntax

clear hsgw-service statistics [name *service_name* **] [| { grep** *grep_options* **| more }]**

name *name*

Clears statistics and counters for a an existing HSGW service name specified as an alphanumeric string of 1 through 63 characters.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear statistics for HSGW services configured on the system.

Example

The following command clears statistics for an HSGW service named *hsgw3*:

```
clear hsgw-service statistics name hsgw3
```

clear hss-peer-service

Clears statistic information for Home Subscriber Service (HSS) peer services configured on the system.

Product

MME

Privilege

Operator

Syntax

clear hss-peer-service statistics [service *name* **]**

statistics [service *name* **]**

statistics: Clears HSS peer service statistical information for all HSS peer services configured on the system.
service *name*: Clears HSS peer service statistic information for an existing HSS peer service specified as an alphanumeric string of 1 through 64 characters.

Usage

Use this command to clear statistics for HSS peer services configured on the system.

Example

The following command clears statistics for an HSS peer service named *hss4*:

```
clear hss-peer-servicey statistics service name hss4
```

clear ims-authorization

Clears statistics for all or for a specified IP Multimedia System (IMS) Authorization Service.

Product

GGSN, SCM

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear ims-authorization { policy-control statistics [ ims-auth-service service_name ] |
service statistics [ name service_name ] } [ | { grep grep_options | more } ]
```

ims-auth-service *service_name*

Clears statistics for the IMSA service specified as an alphanumeric string of 1 through 64 characters.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear IMSA Service statistics.

Example

The following command clears IMSA policy-control statistics for an IMSA service named *test_service*:

```
clear ims-authorization policy-control statistics ims-auth-service
test_service
```

clear ip access-group statistics

Clears all interface access control list (ACL) statistics and the context level ACL statistics that have been configured in the current context. Be aware that updating an access list also causes all ip access-groups utilizing the list to be cleared.

Product

PDSN, GGSN ASN-GW

Privilege

Security Administrator, Administrator

Syntax

```
clear ip access-group statistics
```

Usage

Use this command to clear all interface ACL statistics and the context level ACL statistics that have been configured in the current context.

Example

The following command clears the ACL statistics:

```
clear ip access-group statistics
```

clear ip arp

Clears the address resolution protocol (ARP) cache for a given IP address.

Product

All

Privilege

Security Administrator, Administrator

Syntax

clear ip arp *ip_address*

ip_address

Specifies the IP address for which to clear the ARP cache in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Clear the ARP cache when network changes have occurred for the case where the cached data may cause undue overhead in routing packets.

Example

The following command clears the ARP cache for the IP address *10.2.3.4*:

```
clear ip arp 10.2.3.4
```

clear ip bgp peer

Resets Border Gateway Protocol (BGP) connections for all peers or for specified peers in the current context.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

clear ip bgp peer { *ip_address* | all | as *as_num* } [in | out | soft | vpnv4]

ip_address

Specifies the IP address of the neighbor for which BGP connections should be reset in IPv4 dotted-decimal notation.

all

Resets BGP connections for all peers.

as *as_num*

Resets BGP connections for all peers in the specified autonomous system (AS). *as_num* must be an integer from 1 through 65535.

in

Softly reconfigures inbound updates.

out

Softly reconfigures outbound updates.

soft

Softly reconfigures inbound and outbound updates.

vpnv4

Clears BGP sessions within the vpnv4 address family.

Usage

Use this command to BGP information for the current context.

Example

The following command resets BGP connections for all neighbors:

```
clear ip bgp peer all
```

clear ip localhosts

Removes the host specified from the current context's local host list for IP address mappings.

Product

All

Privilege

Security Administrator, Administrator

Syntax

clear ip localhosts [*host_name* **]**

host_name

Specifies the name of the host to be removed as an alphanumeric string of 1 through 127 characters. When omitted, all local host name mappings will be removed.

Usage

Clears a host name when it is no longer valid for the current context to access. The host name specified will be unrecognized by the current context once the command is performed.

Example

```
clear ip localhosts

clear ip localhosts 10.2.3.4

clear ip localhosts remoteABC
```

clear ip ospf process

Clears Open Shortest Path FIrst (OSPF) database information for the current context and re-establishes neighbor adjacency.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
clear ip ospf process
```

Usage

Use this command to clear the OSPF database information for the current context and re-establishes neighbor adjacency.

Example

The following command clears the OSPF database information for the current context and re-establishes neighbor adjacency:

```
clear ip ospf process
```

clear ipv6 neighbors

Clears an IPv6 address from the neighbor cache.

Product

PDIF

Privilege

Administrator, Security Administrator

Syntax

clear ipv6 neighbors *ip_address*

ip_address

Specifies the IP address in IPv6 colon-separated notation.

Usage

Clears a specific address from the neighbor cache.

Example

Use the following example to clear *3ffe:ffff:101::230:6eff:fe04:d9aa/48*:

```
clear ipv6 neighbors 3ffe:ffff:101::230:6eff:fe04:d9aa/48
```

clear ipv6 ospf process

Restarts Open Shortest Path First Version 3 (OSPFv3) with available configuration.

Product

PDSN, HA GGSN

Privilege

Administrator, Security Administrator

Syntax

```
clear ipv6 ospf process
```

Usage

Force a restart of OSPFv3 process using the available configuration.

Example

```
clear ipv6 ospf process
```

clear l2tp

Clears all or specific Layer 2 Tunnelling Protocol (L2TP) statistics or clears and disconnects all or specified sessions or tunnels.

Product

PDSN, GGSN, LNS

Privilege

Security Administrator, Administrator, Operator

Syntax

clear l2tp { statistics [lac-service *service_name* **| lns-service** *service_name* **| peer-address** *ip_address* **] | tunnels { all [clear-sa] | callid call_id | lac-service** *service_name* **[clear-sa] | lns-service** *service_name* **| peer-address** *ip_address* **[clear-sa] } }**

statistics [lac-service *service_name* **| lns-service** *service_name* **| peer-address** *ip_address* **]**

With no optional keywords specified, this command clears all L2TP statistics for the current context.
lac-service *service_name*: Clears all L2TP statistics for the specified LAC service in the current context.
lns-service *service_name*: Clears all L2TP statistics for the specified LNS service in the current context.
peer-address *ip_address*: Clears all L2TP statistics for the destination (peer LNS) at the specified IP address. The IP address is entered using IPv4 dotted-decimal notation.

tunnels { all [clear-sa] | callid *call_id* **| lac-service** *service_name* **[clear-sa] | peer-address** *ip_address* **[clear-sa] }**

all: Clears all tunnels in the current context.
lac-service service_name: Clears all tunnels in the current context that belong to the specified LAC service and closes the tunnels.
lns-service service_name: Clears all tunnels in the current context that belong to the specified LNS service and closes the tunnels.
peer-address ip_address: Clears all tunnels in the current context whose destination (peer LNS) is the system at the specified IP address. The IP address is specified using IPv4 dotted-decimal notation.
callid call_id: Uses the unique identifier that specifies a particular tunnel in the system to clear that tunnel and disconnect it. The output of the command **show l2tp tunnels** contains a field labeled Callid Hint which lists the call id information to use with this command. This is an 8-byte hexadecimal number.
clear-sa: If any security associations have been established they are cleared.

Usage

Clear L2TP all or specific L2TP statistics or clear sessions in a tunnel and disconnect the tunnel.

Example

To clear all L2TP statistics for the current context, use the following command:

```
clear l2tp statistics
```

To clear all L2TP statistics for the LAC service named *lac1*, use the following command:

```
clear l2tp statistics lac-service lac1
```

Use the following command to clear L2TP statistics for the LNS peer at the IP address *10.10.10.100*:

```
clear l2tp statistics peer-address 10.10.10.100
```

The following command clears and closes all tunnels in the current context:

```
clear l2tp tunnels all
```

The following command clears and closes all tunnels for the LAC service named *lac2*:

```
clear l2tp tunnels lac-service lac2
```

The following command clears and closes all tunnels the peer at the IP address *10.10.10.110*:

```
clear l2tp tunnels peer-address 10.10.10.110
```

clear lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

clear llc statistics

Deletes collected traffic statistics for the GPRS logical link-control (LLC) layer.

Product

SGSN

Privilege

Inspector

Syntax

clear llc statistics [gprs-service *srvc_name* **] [| { grep grep_options | more }]**

gprs-service *srvc_name*

Clears the collected statistics for an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

| grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference*.

Usage

This command deletes statistics collected for the traffic that has gone through the LLC layer for either all GPRS services or for a specified GPRS service.

Example

The following command deletes all LLC statistics for GPRS service *gprs1*:

```
clear llc statistics gprs-service gprs1
```

clear lma-service statistics

Clears Local Mobility Anchor (LMA) statistics and counters found in **show** command outputs and bulk statistics associated with all LMA services or a specific service defined by the parameter in this command.

Product

P-GW

Privilege

Operator

Syntax

clear lma-service statistics [name *service_name* **]**

name *service_name*

Clears statistics and counters for an existing LMA service name specified as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to clear statistics and counters in show command outputs and bulk statistics for all LMA services or for a specific LMA service.

Example

The following command clears statistics and counters for an LMA service named *lma3*:

```
clear lma-service statistics name lma3
```

clear local-policy

Clears local Quality of Service (QoS) policy service statistics and counters found in **show** command outputs and bulk statistics associated with all local QoS policy services or a specific service defined by the parameter in this command.

Product

P-GW

Privilege

Operator

Syntax

clear local-policy statistics [service *service_name* **]**

service *service_name*

Clears statistics and counters for an existing local policy service name specified as an alphanumeric string of 1 through 64 characters.

Usage

Use this command to clear statistics and counters in **show** command outputs and bulk statistics for all local QoS policy services or a specific service.

Example

The following command clears statistics and counters for a local QoS policy service named *lp3*:

```
clear local-policy statistics service lp3
```

clear local-user

Clears information pertaining to local-user administrative accounts.

Product

All

Privilege

Security Administrator

Syntax

clear local-user { database [-noconfirm] | statistics | username *name* **lockout }**

clear local-user database

Clears the local-user database by deleting all information for all local-user accounts.

Caution: Use this command only in the event of security concerns or to address concerns of the local-user account database integrity.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

clear local-user statistics

Clears statistics pertaining to local-user accounts.

clear local-user userame *name* **lockout**

Removes lockouts associated with the local-user account expressed as an alphanumeric string of 3 through 16 characters that is case sensitive.

Usage

This command can be used to remove local-user account lockouts, reset local-user-related statistics to 0, or to delete the local-user database.

Example

The following command removes the lockout placed on a local-user account named *SecureAdmin*:

```
clear local-user username SecureAdmin lockout
```

clear mag-service statistics

Clears Mobile Access Gateway (MAG) statistics and counters found in **show** command outputs and bulk statistics associated with all MAG services or a specific service defined by the parameter in this command.

Product

HSGW, S-GW

Privilege

Operator

Syntax

clear mag-service statistics [name *service_name* **]**

name *service_name*

Clears statistics and counters for an existing MAG service name specified as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to clears statistics and counters in show command outputs and bulk statistics for all MAG services or for a specific MAG service.

Example

The following command clears statistics and counters for a MAG service named *mag1*

```
clear mag-service statistics name mag1
```

clear maximum-temperatures

Clears information pertaining to component maximum temperatures.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear maximum-temperatures
```

Usage

Reset the timestamp to the current time and clear previous maximum temperatures for all temperature monitored components. This may be useful when preparing to study system performance, monitor usage, or trouble shoot the administrative interfaces.

Example

The following command resets the maximum temperature statistics for all monitored chassis components.

```
clear maximum-temperatures
```

clear mipfa statistics

Clears the statistics for the mobile IP foreign agent (MIPFA). The statistics for a specific foreign agent service may be cleared by an explicit command.

Product

PDSN, GGSN,ASN-GW

Privilege

Security Administrator, Administrator, Operator

Syntax

clear mipfa statistics [fa-service *name* **| peer-address** *ip_address* **]**

fa-service *name* **| peer-address** *ip_address*

fa-service *name*: Clears the statistics for an existing FA service specified as an alphanumeric string of 1 through 63 characters. “Total sessions” counters for all peers associated with the service are also reset.
peer-address *ip_address*: Clears the statistics for the peer IP address specified in IPv4 dotted-decimal notation. “Total sessions” counter for the specified peer is also reset.

Usage

Clear all statistics for the MIP foreign agent or for a specific service. This may be useful in monitoring performance and troubleshooting as the statistics may be cleared at a well known time and then collected and transferred for review.

Example

The following clears all statistics for the mobile IP foreign agent.

```
clear mipfa statistics
```

The following commands clear the statistics for the example service only.

```
clear mipfa statistics fa-service sampleService
```

```
clear mipfa statistics peer-address 10.2.3.4
```

clear mipha statistics

Clears the statistics for the mobile IP home agent (MIPHA). The statistics for a home agent service may be cleared by explicit command.

Product

HA

Privilege

Security Administrator, Administrator, Operator

Syntax

clear mipha statistics [ha-service *name* **| peer-address** *ip_address* **]**

ha-service *name* **| peer-address** *ip_address*

ha-service *name*: Clears the statistics for an existing HA service name specified as an alphanumeric string of 1 through 63 characters. "Total sessions" counters for all peers associated with the service are also reset.
peer-address *ip_address*: Clears the statistics for an IP address specified using IPv4 dotted-decimal notation. "Total sessions" counter for the specified peer is also reset.

Usage

Clear all statistics for the MIP home agent or for a specific service. This may be useful in monitoring performance and troubleshooting as the statistics may be cleared at a well known time and then collected and transferred for review.

Example

The following clears all statistics for the mobile IP foreign agent.

```
clear mipha statistics
```

The following command clears the statistics for the example service only.

```
clear mipha statistics ha-service sampleService
```

```
clear mipha statistics peer-address 10.2.3.4
```

clear mme-service db record

Clears the MME database records all instances of session manager running for an MME service filtered with IMSI or GUTI as criteria.

Product

MME

Privilege

Inspector

Syntax

clear mme-service db record { all | guti plmn *plmn_id* **group-id** *mme_grp_id* **code** *mme_code* **m-tmsi** *mtmsi_value* **| imsi** *imsi_identifier* **| instance** *instance_id* **}**

all

Clears all detached database records.

guti plmn *plmn_id* **group-id** *mme_grp_id* **code** *mme_code* **m-tmsi** *mtmsi_value*

This set of keywords specifies the filter criteria as a Globally Unique Temporary Identifier (GUTI) to clear the database records for MME service.
The GUTI is constructed from the GUMMEI and the M-TMSI where GUMMEI is constructed from PLMN (MMC and MNC) *plmn_id* and MME Identifier is constructed from an MME Group ID (MMEGI) *mme_grp_id* and an MME Code (MMEC) *mme_code*.
Within the MME, the mobile is identified by the M-TMSI *mtmsi_value*

imsi *imsi_identifier*

Specifies the filter criteria as International Mobile Subscriber Identity (IMSI) to clear the database records of a session instance. *imsi_identifier* is a 15-character IMSI field that identifies the subscriber's home country and carrier.

instance *instance_id*

Clears all detached database records in an existing session manager instance specified as an integer from 1 through 4294967295.

Usage

Use this command to clear/remove database records for all or a particular instance of session manager for MME services on this system.

Example

The following command clears the summary database records of a session instance for subscriber having IMSI as *123455432112345* in the MME service:

```
clear mme-service db record imsi 123455432112345
```

clear mme-service db statistics

Clears the MME database statistics for MME sessions for all or specific session instances on this system.

Product

MME

Privilege

Inspector

Syntax

clear mme-service db statistics [instance *smgr_instance* **]**

instance *smgr_instance*

Specifies that MME database statistics for a specific instance of session manager running for MME service are to be remove. The instance ID expressed is an integer from 0 through 4294967295. If an instance is not specified, database statistics of all instances will be removed.

Usage

Use this command to clear/remove database statistics for all or a particular instance of session manager for MME services on this system.

Example

The following command removes/clears the database statistics of all instances of the MME service on a system:

```
clear mme-service db statistics
```

clear mme-service statistics

Clears the service statistics of an MME service specified by various criteria.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

```
clear mme-service statistics [ emm-only | esm-only | handover | mme-service mme_svc_name
[ emm-only | esm-only | s1ap | sctp ] | peer-id peer_identifier [ emm-only | esm-only |
s1ap | sctp ] | s1ap | sctp  ]
```

emm-only

Clears all EPS mobility management (EMM) related statistics for a specific MME service name, a specific peer MME identifier, or all EMM statistic instances.

esm-only

Clears all EPS session management (ESM) related statistics for a specific MME service name, a specific peer MME identifier, or all ESM statistic instances.

handover

Clears all handover statistics for this service.

mme-service *mme_svc_name*

Filters by MME service name to clear all service statistics.

peer-id *peer_identifier*

Filters by the identifier of an MME peer to clear all service statistics.

s1ap

Filters by the MME service name of a peer MME identifier to clear all S1-AP statistics.

sctp

Filters by the MME service name of a peer MME identifier to clear all SCTP statistics.

Usage

This command is used to clear the statistical information of an MME service based on various filter criteria.

Example

The following command clears the service session statistics of all MME service on a system:

```
clear mme-service statistics
```

clear multicast-sessions

Disconnects broadcast-multicast sessions based on specified criteria.

Product

PDSN, GGSN

Privilege

Security Administrator Operator

Syntax

clearmulticast-sessions [-noconfirm] [*keywords* **] [verbose]**

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

---

all

Disconnects all multicast sessions.

---

callid *call_id*

Clears the call specified by *call_id*. The call ID is as an 8-byte hexadecimal number.

---

card-num *slot_num*

Specifies the slot number of the packet processing card by which the multicast session is processed as a number from 1 through 7 or 10 through 16.

---

flowid *id*

Clears calls for a specific Broadcast/Multicast Service (BCMCS) flow id, specified as a hexadecimal numbe.r

---

flowid-type [flow | program]

Clears multicast sessions according to the type of flow.
flow: Clears all multicast sessions for the flow ID type “flow”.
program: Clears all multicast sessions for the flow ID type “program”.

---

mcast-address *ipv4_address*

Clears multicast sessions for a specific multicast address. Must be followed by the IP address of an interface in IPv4 dotted-decimal notation.

---

pcf *ipv4_address*

Clears multicast sessions connected via the packet control function defined by an IP address in IPv4 dotted-decimal notation.

---

pdsn_service *name*

Clears multicast sessions connected to an existing packet data service name.

verbose

Displays as much information as possible. If this option is not specified, the output is the standard level which is the concise mode.

Usage

Clear multicast sessions to aid in troubleshooting the system when no additional subscribers may connect or when a specific service or remote address may be having connection problems. This command may also be useful when preparing for maintenance activities such that connects may be cleared to perform any necessary procedures.

The keywords are filters that modify or filter the criteria for deciding which sessions to clear and are described below. Multiple keywords can be entered on a command line.

When multiple keywords are specified, the multicast sessions deleted must meet the specifications of all of the keywords.

Example

The following command clears the broadcast-multicast sessions having multicast address *10.2.3.4*:

```
clear multicast-sessions mcast-address 10.2.3.4
```

The following command clears the broadcast-multicast session(s) having call id *00004e22*:

```
clear multicast-sessions callid 00004e22
```

clear orbem statistics

Clears the interface statistics for the object request broker element manager (ORBEM) interface.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear orbem statistics
```

Usage

Clear the statistics to reset them to zero for the ORBEM interface. This may be useful when preparing to study system performance, monitor usage, or troubleshoot the administrative interfaces.

Example

The following command resets the statistics for the ORB element manager.

```
clear orbem statistics
```

clear pcc-policy service statistics

Clears statistical information of all or a specific policy control and charging (PCC) service configured in a context.

Product

IPCF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

clear pcc-policy statistics [**name** *pcc_plcy_svc_name*

name *pcc_plcy_svc_name*

Clears information only for an existing PCC-Policy service in the current context, expressed as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to clears the statistical information of all or an specific PCC-Policy services configured in a context.
Clearing of statistics can further be filtered for specific PCC-Policy service name as well.

Example

The following command clears the statistical information for the PCC-Policy service named *pcc_policy1* in summarized output:

```
clear pcc-policy service statistics name pcc_policy1
```

clear pcc-policy session

Clears the active/dormant session information about PCC-Policy service instances configured and running on this system based on different filter criteria.

Product

IPCF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

clear pcc-policy sessions [**all**] [**apn** | **call-id** *call_id* | **imsi** *imsi_id* | **ip-address** *pcc_pcef_ip_address* | **service** *pcc_plcy_svc_name*] [**local-purge**]

all

Clears the session information of all registered IP-CAN session(s) on a PCC-Policy service instance running on the system. The display can be filtered based on given filtering criteria.

apn *apn_name*

Clears the session information for PCC-Policy service sessions connected via an existing APN,

imsi *imsi_id*

Clears the session information of IP-CAN session(s) based on the IMSI identifier of a subscriber on a PCC-Policy service instance. *imsi_id* is the International Mobile Subscriber Identity (IMSI) and must be a 15-character field which identifies the subscriber's home country and carrier.

ip-address *pcc_pcef_ip_address*

Clears the session statistics of IP-CAN session(s) based on the registered PCEF (Policy and Charging Enforcement Function) node IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated notation.

call-id *call_id*

Clears the session statistics of IP-CAN session(s) based on the existing registered call id of an IP-CAN session subscriber specified in eight-bye hexadecimal format.

pcc-policy-service *pcc_plcy_svc_name*

Clears the session statistics of registered IP-CAN session(s) based on an existing PCC-Policy service name, expressed as an alphanumeric string of 1 through 63 characters.

local-purge

Clears the session information for PCC-Policy service sessions locally only.

Usage

Use this command to clear the session statistics of all or specific registered IP-CAN session(s) or in selected part of user session for PCC-Policy services configured and running on this system.

Example

The following command clears the session statistics for all registered PCC-Policy service instances on a system/context locally only:

```
clear pcc-policy sessions all local-purge
```

clear pcc-sp-endpoint statistics

Clears the statistical information of all or specific PCC-Sp-Endpoint instance configured in a context.

Product

IPCF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

clear pcc-sp-endpoint statistics [**name** *sp_endpt_name*]

name *sp_endpt_name*

Clears information only for an existing PCC-Sp-Endpoint instance specified as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to clears the statistical information of all or an specific PCC-Sp-Endpoint interface configured in a context.
Clearing of statistics can further be filtered for specific PCC-Sp-Endpoint instance name as well.

Example

The following command clears the statistical information for the PCC-Sp-Endpoint instance named *sp1* in summarized output:

```
clear pcc-sp-endpoint statistics name sp1
```

clear pdg-service statistics

Deletes all previously gathered statistics for a specific Packet Data Gateway (PDG) service or all PDG services configured within a context.

Product

PDG/TTG

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear pdg-service statistics [ name service_name ]
```

name *service_name*

Clears the statistics for the PDG service name configured in the context, expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage

Usage Statistics for a single PDG service can be cleared using the name keyword. Statistics for all PDG services in the context can be deleted by entering the command with no keywords.
If this command is executed from within the local context with no keywords, statistics will be cleared for every PDG service configured on the system regardless of context. In addition, if the name keyword is used when executing from within the local context, statistics for all PDG services configured with the specified name will be cleared regardless of context.

Example

Example(s) The following command clears statistics for a PDG service named *pdg1*:

```
clear pdg-service statistics pdg1
```

clear pgw-service

Clears PDN Gateway (P-GW) statistics and counters found in **show** command outputs and bulk statistics associated with all P-GW services or a specific service defined by the parameter in this command.

Product

P-GW

Privilege

Operator

Syntax

clear pgw-service statistics [name *service_name* **] [| { grep** *grep_options* **| more }]**

name *service_name*

Clears statistics and counters for an existing P-GW service name, expressed as an alphanumeric string of 1 through 63 characters.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear statistics and counters in show command outputs and bulk statistics for all P-GW services or for a specific P-GW service.

Example

The following command clears statistics and counters for an P-GW service named *pgw5*:

```
clear pgw-service statistics name pgw5
```

clear port

Clears port related statistics.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

clear port { datalink counters { all | *slot/port* } | npu counters { all | *slot/port* [untagged | vlan *tag_id*] }

clear port datalink counters

Clears data link port statistics.

clear port npu counters

Clears statistics for the network processing unit(s).

all

Clears counters for all datalink or NPU ports.

slot/port

Clears the statistics for the specified slot and port number.

untagged

Clears NPU statistics for all ports that do not have a VLAN tag.

vlan *tag_id*

Clears NPU statistics for the port that has a previously configured VLAN tag ID.

Usage

Manually clear the statistics for a specified port. This is useful when preparing to trouble shoot or monitor the system.

Example

The following command clears the data link related statistics for port 1 in slot 17.

```
clear port datalink counters 17/1
```

The following command clears the network processing unit related statistics for port 1 in slot 17.

```
clear port npu counters 17/1
```

The following command clears the network processing unit related statistics for port 10 in slot 5.

```
clear port npu counters 5/10
```

clear ppp statistics

Clears point-to-point protocol (PPP) related statistics. All PPP statistics may be cleared or just those for a specific packet data service may be cleared.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear ppp statistics [ggsn-service *ggsn_name* **| lns-service** *lns_name* **| pcf-address [** *pcf_ip_addr* **| all] | pdsn-service** *pdsn_name* **]**

ggsn-service *ggsn_name*

Clears statistics only for the time the session is connected to the named GGSN service.

lns-service *lns_name*

Clears statistics only for the time the session is connected to the named LNS service.

pcf-address [*pcf_ip_addr* **| all]**

Clears statistics only for the time the session is connected to the specified PCF (Packet Control Function) or for all PCFs. *pcf_ip_addr* must be entered using IPv4 dotted-decimal notation.

pdsn-service *pdsn_name*

Clears statistics only for the named PDSN service.

Usage

Allows you to manually reset PPP statistics when it is desired to have counts begin again from a specific point in time.

Example

The following clears the statistics for all PPP counters and services.

```
clear ppp statistics
```

The following clears only the point-to-point protocol statistics for the service named *sampleService*.

```
clear ppp statistics pdsn-service sampleService
```

clear prepaid 3gpp2 statistics

Clears all of the statistics counters for 3GPP2 Pre-paid accounting. Statistics may be cleared for all services or for an individual service.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear prepaid 3gpp2 statistics { all | { ggsn-service | ha-service | lns-service | pdsn-service } { all | name *service_name* **} }**

all

Clears prepaid statistics for all services.

ggsn-service

Clears statistics for GGSN service(s).

ha-service

Clears statistics for HA service(s).

lns-service

Clears statistics for LNS service(s).

pdsn-service

Clears statistics for PDSN service(s).

{ all | name *service_name* **}**

all: Clears statistics for all services of the specified type.
name *service_name*: Clears statistics for the named service of the specified service type.

Usage

Use this command to clear Pre-paid statistics for a particular named service or for all services.

Example

To clear statistics for a PDSN service name *PDSN1*, enter the following command:

```
clear prepaid 3gpp2 statistics pdsn-service name PDSN1
```

clear prepaid wimax

Clears all of the statistical counters for WiMAX prepaid accounting. Statistics may be cleared for all services or for an individual service.

Product

ASN-GW

Privilege

Operator

Syntax

clear prepaid wimax statistics { all | asngw-service { all | name *service_name* **} | ha-service { all | name** *service_name* **} }**

all

Clears prepaid statistics for all services.

asngw-service

Clears prepaid statistics for ASN-GW service(s).

ha-service

Clears prepaid accounting statistics for HA service(s).

{ all | name *service_name* **}**

all: Clears statistics for all services of the specified type.
name *service_name*: Clears statistics for the named service of the specified service type.

Usage

Use this command to clear prepaid WiMAX accounting statistics for named service or for all services.

Example

The following command clears prepaid WiMAX accounting statistics for an ASN-GW service name *asn1*:

```
clear prepaid wimax statistics asngw-service name asn1
```

clear ps-network statistics

Clears the HNB-Packet Switched (PS) network service associated with an HNB-GW service instance.

Product

HNB-GW

Privilege

Operator

Syntax

clear ps-network statistics [name *cs_svc_name* **| gtpu-only | ranap-only | rtp-only | sccp-only]**

name *ps_svc_name*

Clears the session statistics based on an existing HNB-PS network service name, expressed as an alphanumeric string of from 1 through 63 characters.

gtpu-only

Clears the session statistics for GTP-U traffic only for the specified HNB-PS Network service.

ranap-only

Clears the session statistics for Radio Access Network Application Protocol (RANAP) traffic only for the specified HNB-PS Network service.

sccp-only

Clears the session statistics for Signaling Connection Control Part (SCCP) traffic only for the specified HNB-PS Network service.

Usage

Use this command to clear the session statistics for overall session or in selected part of user session for HNB-CS Network services configured and running on a system.

Example

The following command clears the session statistics for RANAP part of session for the HNB-PS Network service *hnb_PS_1*:

```
clear ps-network statistics name hnb_PS_1 ranap-only
```

clear qos npu stats

Clears information pertaining to NPU QoS priority queue bandwidth allocation and sharing.

Product

GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear qos npu stats inter-subscriber traffic slot *slot_num*

inter-subscriber traffic slot *slot_num*

Clears inter-subscriber traffic statistics for the application or line card installed in the specified slot. *slot_num* indicates the number of the chassis slot in which the card is installed and can be configured to an integer value from 1 through 48.

Usage

Allows you to manually reset statistics pertaining to NPU QoS priority queue bandwidth allocation.

Example

The following command clears statistics for a card installed in chassis slot *3*:

```
clear qos npu stats inter-subscriber traffic slot 3
```

clear radius accounting archive

Clears archived RADIUS accounting messages associated with an AAA group, or all the archived RADIUS accounting messages in the context in which the command is executed depending on the option chosen. The scope of the command is limited to the context in which it is executed (including the local context).

Important: This command is only available in StarOS 8.3 and later. For more information, please contact your local service representative.

Product

All

Privilege

Security Administrator, Administrator

Syntax

clear radius accounting archive { all | radius group *group_name* **} [-noconfirm]**

all

Clears all archived RADIUS accounting messages in the context.

radius group *group_name*

Clears all archived RADIUS accounting messages for the RADIUS group specified as an alphanumeric string of 0 through 64 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to clear the archived RADIUS accounting messages associated with an AAA group, or all the archived RADIUS accounting messages in the context in which the command is executed.

Example

Use the following command to clear all archived RADIUS accounting messages for the group named *test12*.

```
clear radius accounting archive radius group test12
```

clear radius counters

Clears statistics for RADIUS servers or a server group. The statistics for all RADIUS servers or a server group may be cleared.

Product

PDSN, GGSN, ASN-GW, P-GW

Privilege

Security Administrator, Administrator, Operator

Syntax

clear radius counters { all | radius group *group_name* **| server** *ip_address* **[port** *number* **] }**

all | radius group *group_name* **| server** *ip_address* **[port** *number* **]**

all: Clears statistics for all servers.
radius group *group_name*: Clears all configured authentication/accounting servers in the specified RADIUS group. *group_name* must be the name of server group configured in a specific context for authentication/accounting, expressed as an alphanumeric string of 1 through 63 characters.
server *ip_address* **[port** *number* **]**: Clears statistics only for the server specified using IPv4 dotted-decimal or IPv6 colon-separated notation. Optionally, you can specify the port which is to have its RADIUS statistics cleared as an integer from 0 through 65535.

Usage

Clear the statistics to reset them to zero prior to logging or monitoring the system for troubleshooting, performance measurements, etc.

Example

The following command clears the statistics for all RADIUS servers.

```
clear radius counters all
```

The following command resets the statistics only for the server *10.2.3.4*.

```
clear radius counters server 10.2.3.4
```

The following command resets the statistics only for the server group named *star1*.

```
clear radius counters radius group star1
```

clear rohc statistics

Clears statistics and counters collected since the last reload or **clear** command was issued for RObust Header Compression (ROHC) [RFC 3095].

Product

PDSN, ASN-GW, HSGW

Privilege

Administrator, Config-administrator, Operator, Inspector

Syntax

clear rohc statistics [pdsn-service *pdsnsvc_name* **| asngw-service** *asngwsvc_name*

pdsn-service *pdsnsvc_name*

Clears ROHC statistics and counters for the specified PDSN service.

asngw-service *asngwsvc_name*

Clears ROHC statistics and counters for the specified ASN-GW service.

Usage

Use this command to clear ROHC statistics for all services or for a specific PDSN or ASNGW service.

Example

The following command clears ROHC statistics and counters for the PDSN service named *pdsn1*:

```
clear rohc statistics pdsn-service pdsn1
```

clear rp service-option

Clears the radio-packet (R-P) interface service option statistics.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear rp service-option statistics [number *option_num* **| pdsn-service** *pdsn_name* **]**

number *option_num* **| pdsn-service** *pdsn_name*

Default: clears the statistics for all service options and all packet data services.
number *option_num*: Specifies the R-P service option number for which the statistics are to be cleared as an integer from 0 through 1000.
pdsn-service *pdsn_name*: Specifies the PDSN service name for which statistics will be cleared.

Usage

Clear the R-P service option statistics prior to monitoring the system for bench marking or for detecting areas of further research.

Example

The following resets the service option statistics for service option *23* and packet data service *sampleService*, respectively.

```
clear rp service-option statistics number 23

clear rp service-option statistics pdsn-service sampleService
```

clear rp statistics

Clears the radio-packet (R-P) interface statistics. The statistics for a specific packet data server or peer node may be cleared if specified.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear rp statistics [pdsn-service *name* **| peer-address [** *peer_address* **| all]]**

pdsn-service *name* **| peer-address [** *peer_address* **| all]**

Default: clears all R-P associated statistics.
pdsn-service *name*: Specifies the packet data service name that is to have its statistics reset.
peer-address [*ip_address* **| all]**: Specifies that statistics for the specified peer, or all peers, are to be cleared. The *ip_address* must be specified using IPv4 dotted-decimal notation.

Usage

Clear the statistics to prepare for monitoring the system.

Example

The following command resets all the associated statistics for the R-P interfaces.

```
clear rp statistics
```

The following command clears the statistics for the packet data service *sampleService*.

```
clear rp statistics pdsn-service sampleService
```

The following command resets the statistics associated with peer node with IP address *10.2.3.4*.

```
clear rp statistics peer-address 10.2.3.4
```

clear sccp statistics

Clears SS7 Signaling Connection Control Part (SCCP) statistics collected for services that use the SCCP protocol.

Product

SGSN

Privilege

Inspector

Syntax

clear sccp statistics [iups-service *iups_srvc_name* **| map-service** *map_srvc_name* **| sccp-network** *ntwk_index* **[dpc** *dpc* **[ssn** *ssn* **] | global-title-translation { address-map instance** *add_map_inst* **| association instance** *assoc_inst* **} [sessmgr instance** *sessmgr_inst* **]] [| { grep** *grep_options* **| more }]**

iups-service *iups_srvc_name*

Deletes collected SCCP protocol statistics for an existing Iu-PS service in the current context specified as an alphanumeric string of 1 through 63 characters.

map-service *map_srvc_name*

Deletes collected SCCP protocol statistics for an existing MAP service specified as an alphanumeric string of 1 through 63 characters.

sccp-network *ntwk_index*

Deletes collected SCCP protocol statistics for the SSCP network configuration with the a network index specified as an integer from 1 through 12.
The following filters can be added to limit the clearing of SCCP network statistics:

- **dpc** *dpc*: Specifies a differentiated pointcode address to limit the deletion of collected SCCP network statistics to those for the identified destination.
- **ssn** *ssn*: Specifies a subsystem number as an integer from 1 to 255 to limit the deletion of collected SCCP network statistics.
- **global-title-translation address-map instance** *add_map_inst*: Specifies an identified GTT address-map as an integer from 1 to 4096 to limit the deletion of collected SCCP network statistics.
- **global-title-translation association instance** *assoc_inst*: Specifies an identified GTT association as an integer from 1 to 16 to limit the deletion of collected SCCP network statistics.
- **sessmgr instance** *sessmgr_inst*: Specifies an identified session manager instance as an integer from 1 to 384 to limit the deletion of collected SCCP network statistics.

Usage

Use this command to delete all collected SCCP statistics or to delete SCCP statistics for a specified service, SCCP network, or session manager.

Example

The following command deletes all collected SCCP statistics:

```
clear sccp statistics
```

The following command clears all collected SCCP statistics for the IuPS service named *iups-serv1*:

```
clear sccp statistics iups-service iups-serv1
```

clear session disconnect-reasons

Clears the session disconnect reason statistics for all sessions on the system.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear session disconnect-reasons
```

Usage

Sets the counters for session disconnect reasons to zero (0) in preparation for a monitoring or troubleshooting session.

Example

```
clear session disconnect-reasons
```

clear session-event-record statistics

Clears statistics collected during session event module transfers.

Product

S-GW

Privilege

Operator

Syntax

```
clear session-event-record statistics
```

Usage

Use this command to delete all collected session event record statistics.

clear session setuptime

Clears the session setup time statistics for Packet Control Functions (PCFs) or SGSNs. If no keyword is specified the summary statistics displayed by the **show session setuptime** command are cleared.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

clear session setuptime { pcf { *pcf_addr* | all } | sgsn { *sgsn_addr* | all } }

pcf { *pcf_addr* | all }

pcf_addr: Clears the setup time counters for the PCF at the IP address specified in IPv4 dotted-decimal notation.
all: Clears the setup time counters for all PCFs.

sgsn { *sgsn_addr* | all }

sgsn_addr: Clears the setup time counters for the SGSN at the IP address specified in IPv4 dotted-decimal notation.
all: Clears the setup time counters for all SGSNs.

Usage

Sets the counters for session disconnect reasons to zero (0) in preparation for a monitoring or troubleshooting session.

Example

To clear the statistics for the PCF at IP address *192.168.100.10*, enter the following command:

```
clear session setuptime pcf 192.168.100.10
```

clear session subsystem

Clears all session subsystem statistics for the current context.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear session subsystem
```

Usage

Clear the statistics in preparation for a troubleshooting or monitoring session so that the counters are at a well known values.

Example

```
clear session subsystem
```

clear sgsn-fast-path statistics

Clears information related to SGSN fast-path.

Product

SGSN

Privilege

Inspector

Syntax

show sgsn-fast-path statistics [all | smgr-instance *smgr_inst* **] [| { grep** *grep_options* **| more }]**

all

Deletes collected fast-path statistics for all session managers.

smgr-instance *smgr_inst*

Clears collected fast-path statistics for a session manager instance specified as an integer from 1 to 65535.

| grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Please refer to the *Regulating the Command Output* section in this reference for details on the usage of **grep** and **more**.

Usage

Use this command to clear all statistics for SGSN fast-path configurations.

Example

The following command deletes all collected fast-path statistics for all SGSN session managers:

```
clear sgsn-fast-path statistics
```

clear sgsn-map-app

Deletes collected statistics for the SGSN Mobile Application Part (MAP).

Product

SGSN

Privilege

Inspector

Syntax

clear sgsn-map-app statistics [| { grep *grep_options* **| more }]**

clear sgsn-map-app statistics

Clears all collected statistics for the SGSN MAP application.

| grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Please refer to the *Regulating the Command Output* section in this reference for details on the usage of **grep** and **more**.

Usage

Use this command to deleted collected statistics for the SGSN MAP application.

Example

The following command clears all collected SGSN MAP statistics:

```
clear sgsn-map-app statistics
```

clear sgs-service

Clears SGs interface statistics associated with a Visitor Location Register (VLR).

Product

All

Privilege

Operator

Syntax

clear sgs-service { statistics [name *name* **] | vlr-status [service-name** *name* **] [vlr-name** *name* **] }**

---

statistics [name *name* **]**

Clears statistics for all SGs services or a specific SGs service.
name *name*: Clears the statistics for an existing SGs service specified as an alphanumeric string of 1 through 63 characters.

---

vlr-status [service-name *name* **] [vlr-name** *name* **] }**

Clears statistics for all VLRs, a VLR related to a SGs service, or a specific VLR.
service-name *name*: Clears the SGs statistics for an existing VLR specified as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to clear statistics for all SGs services, Visitor Location Registers (VLRS), or a specific SGs service or VLR name.

Example

The following command clears statistics for an SGs service named *sgs2*:

```
clear sgs-service statistics name sgs2
```

clear sgtpc statistics

Clears all SGSN GTP-C (SGTPC) statistics for the current context.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear sgtpc statistics [gsn-address *ipv4_address* **| sgtp-service** *sgtp_srvc_name* **]**

gsn-address *ipv4_address*

Clears GTPC packet statistics for the interface specified as an IP address in IPv4 dotted-decimal notation.

sgtp-service *sgtp_srvc_name*

Clears GTPC packet statistics for an existing SGTP service specified as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to clear the statistics in preparation for a troubleshooting or monitoring session.

Important: Statistics are vital for troubleshooting. We recommend that you check with your Cisco support personnel prior to clearing these statistics.

Example

```
clear sgtpc statistics sgtp-service SGSN1sgtp12
```

clear sgtpu statistics

Clears all SGSN GTP-U (SGTPU) statistics for the current context.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear sgtpu statistics [ggsn-address *ipv4_address* **| gprs-service** *gprs_srvc_name* **nsei** *nse_id* **| iups-bind-address** *ipv4_address* **| iups-service** *iups_srvc_name* **| rnc-address** *ipv4_address* **| sgtp-service** *sgtp_srvc_name* **]**

ggsn-address *ipv4_address*

Clears GTPU packet statistics for a specific GGSN specified as an IP address in IPv4 dotted-decimal notation.

gprs-service *gprs_srvc_name* **nsei** *nse_id*

gprs-service *gprs_srvc_name*: Clears GTPU packet statistics for the interface for a specific GPRS service specified as an alphanumeric string of 1 through 63 characters.
nsei *nse_id*: Specifies a network service entity (NSEI) as an integer from 0 through 65535.

iups-bind-address *ipv4_address*

Clears GTPU packet statistics for the bind address of an IuPS interface specified as an IP address in IPv4 dotted-decimal notation.

iups-service *iups_srvc_name*

Clears GTPU packet statistics for an active IuPS service interface specified as an alphanumeric string of 1 through 63 characters.

rnc-address *ipv4_address*

Clears GTPU packet statistics for an RNC specified as an IP address in IPv4 dotted-decimal notation.

sgtp-service *sgtp_srvc_name*

Clears GTPU packet statistics for an active SGTP service interface specified as n alphanumeric string of 1 through 63 characters.

Usage

Use this command to clear the statistics in preparation for a troubleshooting or monitoring session.

Important: Statistics are vital for troubleshooting. We recommend that you check with your Cisco support personnel prior to clearing these statistics.

Example

Use this command to clear collected SGTPU statistics for a specific NSEI of a configured GPRS service:

```
clear sgtpu statistics gprs-service SGSN1Gprs1 nsei 2445
```

clear sgw-service statistics

Clears Serving Gateway (S-GW) statistics and counters found in **show** command outputs and bulk statistics associated with all S-GW services or a specific service defined by the parameter in this command.

Product

S-GW

Privilege

Operator

Syntax

clear sgw-service statistics { all | name *service_name* **}**

all

Clears statistics and counters for all S-GW services configured on the system.

name *service_name*

Clears statistics and counters for an existing S-GW service name specified as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to clears statistics and counters in show command outputs and bulk statistics for all S-GW services or for a specific S-GW service.

Example

The following command clears statistics and counters for an S-GW service named *sgw3*:

```
clear sgw-service statistics name sgw3
```

clear sms statistics

Deletes collected traffic statistics for the Short Message Service (SMS).

Product

SGSN

Privilege

Administrator, Security Administrator, Operator

Syntax

clear sms statistics [name *map_srvc* **] [| { grep** *grep_options* **| more }]**

name *map_srvc*

Specifies a MAP Service as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to delete collected traffic statistics for SMS. It is possible to clear the statistics of a specific MAP service associated with the SMS by including the **name** filter.

Example

Use the following command to clear SMS statistics for MAP service *MAP-LONDON1*:

```
clear sms statistics name MAP-LONDOND1
```

clear sndcp statistics

Deletes all collected statistics for the packet traffic going through the Subnetwork Dependent Convergence Protocol (SNDCP) layer.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear sndcp statistics [ gprs-service srvc_name ] [ | { grep grep_options | more } ]
```

gprs-service *srvc_name*

Specifies a GPRS service as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to delete all collected SNDCP traffic statistics. Include the **gprs-service** keyword to filter the clearing action to only deleted statistics for one GPRS service.

Example

Use the following command to clear all collected SNDCP layer traffic statistics:

```
clear sndcp statistics
```

Use the following command to delete SNDCP layer traffic statistics for the *test1* GPRS service:

```
clear sndcp statistics gprs-service test1
```

clear snmp trap

Clears all SNMP event trap notifications from the buffer.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear snmp trap { history | statistics }
```

history

Clears all SNMP historical trap information from the system buffer.

statistics

Clears all SNMP event trap information from the system buffer.

Usage

Use this command to empty the buffer of all SNMP trap notifications.

Example

The following command clears the all historical SNMP traps from the system buffer:

```
clear snmp trap history
```

clear srp

Clears system Service Redundancy Protocol (SRP) statistics.

Product

All products that support Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear srp { audit-statistics | call-loss statistics | checkpoint statistics | statistics
}
```

audit-statistics

Clears SRP audit statistics.

call-loss statistics

Clears SRP call loss history.

checkpoint statistics

Clears SRP checkpoint interface statistics.

statistics

Clears SRP statistics.

Usage

Clears the SRP statistics to prepare the system for SRP monitoring.

Example

The following command resets all the associated statistics for SRP checkpoints.

```
clear srp checkpoint statistics
```

The following command resets all the associated statistics for SRP.

```
clear srp statistics
```

clear ssl statistics

Deletes all previously gathered Secure Sockets Layer (SSL) statistics for a specific P-CSCF service or all P-CSCF services, either system-wide or within a context.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear ssl statistics [ service-name name ]
```

service-name *name*

Specifies the name of a P-CSCF service for which to clear SSL statistics as an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage

SSL statistics for a single P-CSCF service can be cleared using the **service-name** keyword. SSL statistics for all P-CSCF services can be deleted by entering the command with no keywords.
If this command is executed from within the local context with no keywords, SSL statistics will be cleared for every P-CSCF service configured on the system regardless of context. In addition, if the **service-name** keyword is used when executing from within the local context, SSL statistics for all P-CSCF services configured with the specified name will be cleared regardless of context.

Example

The following command clears SSL statistics for the P-CSCF service *pcscf_service_1*:

```
clear ssl statistics service-name pcscf_service_1
```

clear subscribers

Disconnects subscribers based on specified criteria.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

clear subscribers [*keywords* **] [verbose] [-noconfirm]**

The keywords are filters that modify or filter the criteria for deciding which subscriber sessions to clear and are described below. Multiple keywords can be entered on a command line.
When multiple keywords are specified, the subscriber sessions deleted must meet the specifications of all of the keywords.
For example; if you enter the following command:

```
clear subscribers ip-pool pool1 card-num 1
```

Only subscriber sessions that were assigned an IP address from the IP pool named *pool1* and are also being processed by the processing card in slot *1* are cleared. All other subscriber sessions that do not meet these criteria remain and are not cleared.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Important: The Operator privilege does not have access to this keyword.

active

Only disconnects subscribers who currently have active sessions.

active-charging-service *ecs_service_name*

Clears information for subscribers using the Active charging Service.
ecs_service_name must be the name of the Active Charging Service, expressed as an alphanumeric string of 1 through 15 characters.

all

Disconnects all subscribers.

Important: The Operator privilege does not have access to this keyword.

apn *name*

Clears all PDP contexts accessing a specific access point name (APN).
apn_name is the name of the APN expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

asn-peer-address *ip_address*

Clears information for subscribers on an ASN-GW trusted peer.
ip_address is the address of the ASN-GW peer server entered using IPv4 dotted-decimal notation.

asngw-service *service_name*

Clears counters for subscribers accessing the ASN-GW service.
service_name must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

asnpc-service *service_name*

Clears counters for subscribers accessing the ASN PC service.
service_name must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

bandwidth-policy *bandwidth_policy_name*

Clears information for subscribers using the specified bandwidth policy.
bandwidth_policy_name must be the name for an existing bandwidth policy, expressed as an alphanumeric string of 1 through 63 characters.

callid *id*

Clears the call specified by *call_id*. The call ID must be specified as a 4-byte hexadecimal number.

card-num *card_num*

The slot number of the processing card by which the subscriber session is processed. *card_num* is a slot number from 1 through 7 or 10 through 16.

cbb-policy *cbb_policy_name*

Clears information for subscribers using the specified CBB policy.
cbb_policy_name must be the name for an existing CBB policy expressed as an alphanumeric string of 1 through 63 characters.

ccoa-only

This option clears the subscribers that registered a MIP co-located COA directly with the HA.
This option is only valid when MIPHA session license is enabled.

configured-idle-timeout [< | > | greater-than | less-than] *value*

Disconnects subscribers whose idle timeout matches the specified criteria. A value of 0 (zero) indicates that the subscribers idle timeout is disabled.
<: Filters output so that only information less than the specified value is cleared.
>: Filters output so that only information greater than the specified value is cleared.
greater-than: Filters output so that only information greater than the specified value is cleared.
less-than: Filters output so that only information less than the specified value is cleared.
value: If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 4294967295.

connected-time [< | > | greater-than | less-than] *value*

Disconnects subscribers who have been connected for the specified length of time.
<: Filters output so that only information less than the specified value is cleared.
>: Filters output so that only information greater than the specified value is cleared.

greater-than: Filters output so that only information greater than the specified value is cleared.
less-than: Filters output so that only information less than the specified value is cleared.
value: If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 4294967295.

---

cscf-service *service_name*

Clears all subscribers from the specified CSCF service.
service_name must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

---

css-delivery-sequence *name*

Important: This is a restricted keyword. In StarOS 9.0 and later, this keyword is obsoleted.

---

css-service *name*

Important: This is a restricted keyword. In StarOS 9.0 and later, this keyword is obsoleted.

---

dhcp-server *address*

Clears all PDP contexts that currently possess an IP address assigned from a specific DHCP server.
dhcp_address is the IP address of the DHCP server expressed in IPv4 dotted-decimal notation.

---

dormant

Only disconnects subscriber sessions that are dormant (not transmitting or receiving data).

---

ebi *number*

Clears subscribers based on an EPS bearer identity (EBI). *number* must be a valid EBI and an integer value from 5 to 15.

---

enodeb-address *ip_address*

Clears subscribers based on the eNodeB to which they are attached. *ip_address* must be a valid IP address of an existing eNodeB entered using IPv4 dotted-decimal or IPv6 colon-separated notation.

---

fa *ip_address*

Disconnects all subscribers connected to the foreign agent specified by the IP address in IPv4 dotted-decimal notation.

---

fa-service *fa_name*

Disconnects all subscribers connected to an existing foreign agent name.

---

firewall { not-required | required }

Clears all subscriber information for the specified subscribers:
not-required: Subscribers for whom firewall processing is not-required.
required: Subscribers for whom firewall processing is required.

firewall-policy *fw_policy_name*

This keyword is obsolete.

fw-and-nat policy *fw&nat_policy_name*

Clears information for subscribers using the specified Firewall-and-NAT policy.
fw&nat_policy_name must be the name of an existing Firewall-and-NAT policy expressed as an alphanumeric string of 1 through 63 characters.

fng-service *service_name*

Clears subscriber sessions connected to the FNG service. *service_name* must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

ggsn-service *name*

Clears all PDP contexts accessing an existing GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

gprs-service *name*

Clears all PDP contexts associated with the 2G SGSN. This keyword can be used with filtering keywords that are part of the **clear subscriber** command set.
Using this keyword can trigger a network-initiated service request (paging) procedure.
name identifies a specific GPRS service configuration expressed as an alphanumeric string of 1 through 63 characters.

gsm-traffic-class { background | conversational | interactive { *priority* **} | streaming }**

Subscribers whose traffic matches the specified 3GPP traffic class.

- **background**: 3GPP QoS background class.
- **conversational**: 3GPP QoS conversational class.
- **interactive**: 3GPP QoS interactive class. Must be followed by a traffic priority. priority can be configured to any integer value from 1 to 3.
- **streaming**: 3GPP QoS streaming class.

gtp-version

Displays the specific GTP version number. Must be followed by one of the supported GTP versions (0 or 1).
The following filter keywords are valid with this command:
active-charging-service, apn, asngw-service, asnpc-service, asn-peer-address, bearer-establishment, callid, card-num, coaa-only, configured-idle-timeout, connected-time, cscf-service, dhcp-server, fa, fa-service, firewall, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, ha, ha-ipsec-service, ha-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, plmn-type, rulebase, rx-data, session-time-left, sgsn-address, sgsn-service, tx-data, username, grep, more

ha *address*

Disconnects all subscribers connected to the home agent specified by *ha_address* must be specified using IPv4 dotted-decimal notation.

ha-ipsec-only

Disconnects all MIP HA sessions with IPSec tunnels.

ha-service *name*

Disconnects all subscribers connected to the home agent specified by *ha_name* must have been previously defined.

hsgw-service *name*

Disconnects subscribers using this HRPD Serving Gateway (HSGW) service configured on this system. *name* must be an existing HSGW service expressed as an alphanumeric string of 1 through 63 characters.

idle-time [< | > | greater-than | less-than] *value*

Disconnects subscribers whose idle time matches the specified length of time.
<: Filters output so that only information less than the specified value is cleared.
>: Filters output so that only information greater than the specified value is cleared.
greater-than: Filters output so that only information greater than the specified value is cleared.
less-than: Filters output so that only information less than the specified value is cleared.
value: If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 4294967295.

ims-auth-service *imsa_service_name*

Disconnects subscribers using this IMS Authorization Service configured on this system.
imsa_service_name must be an existing IMS Authorization Service expressed as an alphanumeric string of 1 through 63 characters.

imsi *id*

Disconnects the subscriber with the specified id. The IMSI (International Mobile Subscriber Identity) ID is a 50-bit field which identifies the subscriber's home country and carrier. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘). For example; ‘$’.

ip-alloc-method {aaa-assigned | dhcp [relay-agent | proxy-client] | dynamic-pool | l2tp-lns-assigned | mip-ha-assigned | ms-provided-static | not-ms-provided-static | static pool }

Displays the specific IP Allocation Method. Must be followed by one of the IP Allocation Methods:

- **aaa-assigned**: Selects subscribers whose IP Addresses were assigned by AAA.
- **dhcp**: Selects subscribers whose IP Addresses were assigned by DHCP.
- **relay-agent**: Selects subscribers whose IP Addresses were assigned by the DHCP Relay Agent
- **proxy-client**: Selects subscribers whose IP Addresses were assigned by the DHCP Proxy Client
- **dynamic-pool**: Selects subscribers whose IP Addresses were assigned from a dynamic IP address pool.
- **l2tp-lns-assigned**: Selects subscribers whose IP Addresses were assigned by the Layer 2 Tunnelling Protocol Network Server.
- **mip-ha-assigned**: Selects subscribers whose IP Addresses were assigned by the Mobile IP Home Agent.

- **ms-provided-static**: Selects subscribers whose IP Addresses were provided by the Mobile Station.
- **not-ms-provided-static**: Selects subscribers whose IP Addresses were not provided by the Mobile Station.
- **static-pool**: Selects subscribers whose IP Addresses were assigned from a static IP address pool.

---

ip-address *address*

Disconnects all subscribers connected to the specified *ip_address*. The address must be specified using IPv4 dotted-decimal notation.

---

ip-pool *name*

Disconnects all subscribers assigned addresses from the IP address pool *pool_name*. *pool_name* must be the name of an existing IP pool or IP pool group.

---

ipv4

Clears all subscribers with IPv4 Firewall enabled/disabled.

---

ipv6

Clears all subscribers with IPv6 Firewall enabled/disabled.

---

ipv6-address *address*

Clears all subscribers connected to the specified IPv6 *address*.

---

ipv6-prefix *prefix*

Clears subscribers from a specific IPv6 address prefix.

---

lac *address*

Disconnects all calls to the peer LAC (L2TP access concentrator) specified by *address* must be specified using IPv4 dotted-decimal notation.

---

lac-service *name*

Disconnects all calls for this LAC service. *name* is an alphanumeric string of 1 through 63 characters.

---

lma-service *name*

Disconnects subscribers using this LMA service configured on this system. *name* must be an existing LMA service expressed as an alphanumeric string of 1 through 63 characters.

---

lns *address*

Disconnects calls to the peer LNS (L2TP network server) specified by *address* must be specified using IPv4 dotted-decimal notation.

---

lns-service *name*

Disconnects calls associated with the LNS service named *name*. *name* is an alphanumeric string of 1 through 63 characters.

long-duration-time-left [< | > | greater-than | less-than] *value*

Disconnects subscriber sessions whose time left for the maximum duration of their session matches the length of time specified.
<: Filters output so that only information less than the specified value is cleared.
>: Filters output so that only information greater than the specified value is cleared.
greater-than: Filters output so that only information greater than the specified value is cleared.
less-than: Filters output so that only information less than the specified value is cleared.
value: If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 4294967295.

mag-service *name*

Disconnects subscribers using this Mobile Access Gateway (MAG) service configured on this system. *name* must be an existing MAG service and be from 1 to 63 alphanumeric characters.

mip-udp-tunnel-only

This option clears the subscribers that negotiated MIP-UDP tunneling with the HA.
This option is only valid when MIP NAT Traversal license is enabled.

mme-address *ipv4_addr*

Disconnects subscribers using this peer Mobility Management Entity (MME). *ipv4_addr* must be an existing peer MME IP address entered using IPv4 dotted-decimal notation.

mme-only

Disconnects all MME subscriber sessions on the system.

mme-service *name*

Disconnects subscribers using this MME service configured on this system. *name* must be an existing MME service expressed as an alphanumeric string1 through 63 characters.

mseg-only

Important: This keyword is not supported in this release. For more information please contact your Cisco account representative.

Clears subscriber information for all MSEG service subscribers.

mseg-service *mseg_service_name*

Important: This keyword is not supported in this release. For more information please contact your Cisco account representative.

Clears subscriber information for subscribers using the specified MSEG service.
mseg_service_name must be name of an existing MSEG service expressed as an alphanumeric string of 1 through 63 characters.

msid *id*

Disconnects the mobile user identified by *ms_id*. *ms_id* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘). For example; ‘$’.
In case of **enforce imsi-min equivalence** is enabled on the chassis and MIN or IMSI numbers supplied, this filter will clear subscribers with a corresponding MSID (MIN or IMSI) whose lower 10 digits matches to lower 10 digits of the supplied MSID.
clear subscribers msid *111110123456789* or
clear subscribers msid *0123456789*
will clear any subscriber with a MSID that match the lower 10 digits of MSID supplied, i.e. 0123456789.

msisdn *msisdn*

Clears information for the mobile user identified by Mobile Subscriber ISDN Number (MSISDN). *msisdn* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI.

nat { not-required | required [nat-ip *nat_ip_address* **| nat-realm** *nat_realm* **] }**

Clears all subscriber information for the specified subscribers:
not-required: Subscribers for whom NAT processing is not required.
required: Subscribers for whom NAT processing is required.

Important: The **nat-ip** keyword is only available in StarOS 8.3 and later.

nat-ip *nat_ip_address*: Subscribers for whom NAT processing is enabled and are using the specified NAT IP address. *nat_ip_address* specifies the NAT IP address using IPv4 dotted-decimal notation.
nat-realm *nat_realm*: Subscribers for whom NAT processing is enabled and are using the specified NAT realm. *nat_realm* specifies the NAT realm name expressed as an alphanumeric string of 1 through 63 characters.

network-requested

Disconnect subscriber sessions that were initiated by the GGSN network requested create PDP context procedure.

network-type { gre | ipv4 | ipv6 | ipip | l2tp | mobile-ip | proxy-mobile-ip }

Disconnects subscriber sessions based on the network type. The following network types can be selected:

- **gre**: Generic Routing Encapsulation (GRE) per RFC 2784
- **ipv4**: Internet Protocol version 4 (IPv4)
- **ipv6**: Internet Protocol version 6 (IPv6)
- **ipip**: IP-in-IP encapsulation per RFC 2003
- **l2tp**: Layer 2 Tunneling Protocol encryption per RFC 2661
- **mobile-ip**: Mobile IP
- **proxy-mobile-ip**: Proxy Mobile IP

pcf [< | > | less-than | greater-than] *ipv4_address* **[[< | > | less-than | greater-than]** *ipv4_address* **]**

Displays information for subscribers connected via the packet control function with a specific or range of IP address *ipv4_ddress*. The address must be specified using IPv4 dotted-decimal notation.

- **<**: Filters output so that only information less than the specified IPv4 address value is displayed.
- **>**: Filters output so that only information greater than the specified IPv4 address value is displayed.
- **less-than**: Filters output so that only information less than the specified IPv4 address value is displayed.
- **greater-than**:Filters output so that only information greater than the specified IPv4 address value is displayed.

Note: It is possible to define a limited range of IP addresses by using the less-than and greater-than options to define minimum and maximum values.

pdsn-service *name*

Disconnect all subscribers connected to the packet data service *pdsn_name*. The packet data service must have been previously configured.

pdg-service *service_name*

Disconnects subscriber sessions that are using the PDG service.
service_name must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

pdif-service *service_name*

Clears counters for subscribers accessing the Packet Data Interworking Function (PDIF) service.
service_name must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

pgw-only { all | imsi *id* **ebi** *id* **| pgw-service** *name* **| sgw-address** *ipv4_addr* **}**

all: Disconnects all subscribers for all P-GW services on this system.
imsi *id* **ebi** *id*: Disconnects subscribers based on their International Mobile Subscriber Identification (IMSI). *id* must be the 3-digit MCC (Mobile Country Code), follow by the 2 or 3 digits of the MNC (Mobile Network Code) and the MSIN (Mobile Subscriber Identification Number). *id* should not exceed 15 digits.
Example: 123-45-678910234 must be entered as 12345678910234
The EBI (EPS Bearer Identity) *id* must be a valid EBI and be an integer value from 5 to 15.
pgw-service*name*: Disconnects all subscribers using this P-GW service. *name* must be an existing P-GW service expressed as an alphanumeric string of 1 through 63 characters.
sgw-address*ipv4_addr*: Disconnects all subscribers using this S-GW IP address. *ipv4_addr* must be an existing IP address entered using IPv4 dotted-decimal notation.

plmn-type { home | roaming |visiting }

For GGSN, disconnects subscribers whose subscriber type matches the specified type.

qci { *number* **}**

Disconnects subscribers based on their QCI identity. *number* must be an integer from 0 to 9.

rulebase *rulebase_name*

Clears information for subscribers using the specified rulebase.

rulebase_name must be name of an existing rulebase expressed as an alphanumeric string of 1 through 63 characters.

---

rx-data [< | > | greater-than | less-than] *value*

Disconnects subscribers who have received the specified number of bytes of data.
<: Filters output so that only information less than the specified value is cleared.
>: Filters output so that only information greater than the specified value is cleared.
greater-than: Filters output so that only information greater than the specified value is cleared.
less-than: Filters output so that only information less than the specified value is cleared.
value: If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 18446744073709551615.

---

s5-proto { gtp | pmip }

Disconnects subscribers based on their S5 interface protocol type.
gtp: Indicates that the GTP protocol is used on the S5 interface for the subscribers being disconnected.
pmip: Indicates that the PMIP protocol is used on the S5 interface for the subscribers being disconnected.

---

session-time-left [< | > | greater-than | less-than] *value*

The amount of time left for the subscriber session.
<: Filters output so that only information less than the specified value is cleared.
>: Filters output so that only information greater than the specified value is cleared.
greater-than: Filters output so that only information greater than the specified value is cleared.
less-than: Filters output so that only information less than the specified value is cleared.
value: If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 4294967295.

---

sgsn-address *address*

Clears all PDP contexts currently being facilitated by a specific SGSN.
address is the IP address of the SGSN entered using IPv4 dotted-decimal notation.

---

sgsn-service *name*

Clears all PDP contexts associated with SGSN. This keyword can be used with filtering keywords that are part of the **clear subscriber** command set.
Using this keyword can trigger a network-initiated service request (paging) procedure.
name identifies a specific SGSN-service configuration expressed as an alphanumeric string of 1 through 63 characters.

---

sgw-only

Disconnects all S-GW subscriber sessions on the system.

---

sgw-service *name*

Disconnects subscribers using this Serving Gateway (S-GW) service configured on this system. *name* must be an existing S-GW service expressed as an alphanumeric string of 1 through 63 characters.

---

tpo { not-required | required }

Clears all subscriber information for the specified subscribers:
not-required: Subscribers for whom TPO processing is not required.
required: Subscribers for whom TPO processing is required.

tx-data [< | > | greater-than | less-than] *value*

Disconnects subscribers who have transmitted the specified number of bytes of data.
<: Filters output so that only information less than the specified value is cleared.
>: Filters output so that only information greater than the specified value is cleared.
greater-than: Filters output so that only information greater than the specified value is cleared.
less-than: Filters output so that only information less than the specified value is cleared.
value: If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. value must be an integer from 0 through 18446744073709551615.

username *name*

Disconnect the subscriber with the specified username
name is the username of the subscriber to be cleared. *name* must be a sequence of characters and/or wildcard characters ('$' and '*') from 1 to 127 characters. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes (‘). For example; ‘$’.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output is the standard level which is the concise mode.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

Usage

Clear subscribers sessions to aid in troubleshooting the system when no additional subscribers may connect or when a specific service or remote address may be having connection problems. This command may also be used to clear connections when preparing for maintenance activities.
Related commands to clear subscription data - *for SGSN use only*

- For a 2G SGSN, the **admin-disconnect-behavior clear-subscription** command in the GPRS Service Configuration mode enables the SGSN to clear subscription data after the administrative disconnect - **clear subscribers all** has been issued.
- For a 3G SGSN, the **admin-disconnect-behavior clear-subscription** command in the SGSN Service Configuration mode enables the SGSN to clear subscription data after the administrative disconnect - **clear subscribers all** has been issued.

Example

The following examples illustrate the basic command usage as well as the redirection of the command output. Not all options are exemplified as all options follow the same basic constructs.
The following are basic subscriber clearing examples.

```
clear subscribers username ser1

clear subscribers ha sampleService

clear subscribers ip-pool pool2 verbose
```

The following command disconnects users connected to the foreign agent with IP address *10.2.3.4*.

```
clear subscribers fa 10.2.3.4
```

clear super-charger

Deletes the subscriber's backed-up subscription data.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
clear super-charger { imsi | all }
```

imsi

Specifies a subscriber's international mobile subscriber identity (IMSI) number. This 15-digit number includes the MCC (mobile country code), the MNC (mobile network code) and the MSIN (mobile station identification number),

all

Instructs the SGSN to delete subscription data for all super charger subscribers.

Usage

Use this command to clear (delete) the subscription data records for one or all subscribers within a super charger subscription configuration.

Example

The following command deletes the backed up records for the subscriber identified by the IMSI *90121882144672*.

```
clear super-charger imsi 90121882144672
```

clear tcap statistics

Deletes the collected statistics for traffic that has passed through the TCAP (Transaction Capabilities Application Part) layer.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

clear tcap statistics [camel-service [all | name *camel_srvc* **] | map-service [all | name** *map_srvc* **]] [| { grep** *grep_options* **| more }]**

camel-service [all | name *camel_srvc* **]**

Deletes TCAP statistics for either all CAMEL (Customized Applications for Mobile Network Enhanced Logic, GSM 09.78) services or only for the named CAMEL service.

map-service [all | name *mapl_srvc* **]**

Deletes TCAP statistics for either all MAP services or only for the named MAP service.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to clear (delete) the collected TCAP statistics for MAP or CAMEL services.

Example

The following command deletes the collected statistics for a MAP service named *MAP-Tewk*.

```
clear tcap statistics map-service name MAP-Tewk
```

cli

Specifies command line interface (CLI) session behavior

Product

All

Privilege

Security Administrator, Administrator, Operator, inspector

Syntax

```
cli { history | stop-on-first-error }

no cli { history | stop-on-first-error }
```

no

Disables the specified keyword functionality.

history

Enables command line history for the current command line session. Default: Enabled

stop-on-first-error

When enabled and a configuration file is loaded, the system stops loading the configuration file on the first syntax error. Default: Disabled

Usage

This command controls CLI settings pertaining to the maintenance of a per-session command history and syntax error monitoring during configuration file loading.
By default, the system maintains a list of commands executed during each CLI session. This list is referred to as a history.
In addition, the system can be configured to stop loading a configuration if a syntax error is detected. By default, the system identifies the error but continues to process the configuration file.

Example

The following command disables the keeping of a CLI history for the current session:

```
no cli history
```

clock set

Sets the system time.

Product

All

Privilege

Security Administrator, Administrator

Syntax

clock set *date_time*

clock set *date_time*

Specifies the date and time to set the system clock in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where:

- YYYY = 4-digit year
- MM = 2-digit month in the range 01 through 12
- DD = 2-digit day in the range 01 through 31
- HH = 2-digit hour in the range 00 through 23
- mm = 2-digit minute in the range 00 through 59
- ss = 2-digit second in the range 00 through 59

Usage

Set the clock to adjust the system clock for such things as timing drift, day-light savings adjustment, etc. New settings are immediately applied to all CPUs in the system.

Important: This command should only be used if there is no NTP server enabled for any context. If NTP is running on the system, this command returns a failure.

Example

The following commands set the system clock where one sets the exact second as well.

```
clock set 2011:08:05:02:30

clock set 2011:08:05:02:31:30
```

configure

Sets the mode to the global configure mode. May also be used to set the mode to the configure mode and pre-load the configuration referred to by the options.

Product

All

Privilege

Security Administrator, Administrator

Syntax

configure [*url* **[verbose]]**

url

Specifies the location of a configuration file to pre-load. *url* may refer to a local or a remote file. *url* must be entered using the following format:

- **[file:]{ /flash | /pcmcia1 | /hd } [/***directory* **]/***file_name*
- **tftp://{** *host***[** *:port#* **] } [/***directory* **]/***file_name*
- **[http: | ftp: | sftp:]//[** *username* **[** *:password***] @] {** *host* **} [** *:port#* **] [/***directory* **]/***file_name*

Important: Use of the SMC hard drive is not supported in this release.

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

verbose

Displays the line number and actual line content from the configuration as it is processed.

Usage

If no URL is specified, executing this command causes the CLI to enter the Global Configuration Mode. If a URL is specified, executing this command loads the specified configuration file.

Example

The following simply changes the mode to the command line interface global configuration mode.

```
configure
```

The following command loads a configuration file from the node *sampleNode* given the path specified and a local file, respectively.

```
configure ftp://sampleNode/pub/glob.cfg

configure /pcmcia1/pub/glob.cfg verbose
```

context

Sets the current context to the context specified.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

context *name*

context *name*

Specifies the context of interest as an alphanumeric string of 1 through 79 characters. Must be a previously defined context.

Usage

Change the current context when it is desired to configure and/or manage a specific context.

Example

The following sets the current context to the *sampleContext* context.

```
context sampleContext
```

copy

Copies files from one location to another. Allows files to be copied to/from locally, as well as from one remote location to another.

Product

All

Privilege

Security Administrator, Administrator

Syntax

copy *from_url to_url* **[passive] [-noconfirm]**

from_url

Specifies the source of the copy. *url* may refer to a local or a remote file. *url* must be entered using the following format:

- **[file:]{ /flash | /pcmcia1 | /hd }[/***directory* **]/***file_name*
- **tftp://{** *host*[*:port#* **] }[/***directory* **]/***file_name*
- **[http: | ftp: | sftp:]//[** *username* **[** *:password* **]@] {** *host* **}[** *:port#* **][/***directory* **]/***file_name*

Important: Use of the SMC hard drive is not supported in this release.

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

to_url

Specifies the destination of the copy. *url* may refer to a local or a remote file. *url* must be entered using the following format:

- **[file:]{ /flash | /pcmcia1 | /hd }[/***directory* **] /***file_name*
- **tftp://{** *host***[** *:port#* **] } [/***directory* **] /***file_name*
- **[ftp: | sftp:] / / [** *username* **[** *:password* **] @] {** *host* **} [** *:port#* **] [/***directory* **] /***file_name*

Important: Use of the SMC hard drive is not supported in this release.

directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

passive

Indicates the file copy is to use the passive mode.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Important: Use of the **-noconfirm** option allows the over writing of an existing file if the destination file already exists.

Usage

Copy configuration files, log files, etc.,to provide backups of data through the network.

Example

The following copies files from the local */flash/pub* directory to remote node *remoteABC*'s */pcmcia2/pub* directory with and without confirmation respectively.

```
copy http://remoteABC/pub/june.cfg /flash/pub/june.cfg

copy tftp://remoteABC/pub/june.cfg /pcmcia2/pub/june.cfg -noconfirm
```

The following copies files from remote node *remoteABC* to remote node *remote123*.

```
copy ftp://remoteABC/pub/may.cfg ftp://remote123/pub/may.cfg
```

crash copy

Copies individual crash files (one-at-a-time) and optionally the core dump file from the stored crash records on the chassis to a user-specified location.

Product

All

Privilege

Security Administrator, Administrator

Syntax

crash copy number *number* **url** *to_url* **[core]**

number *number*

Specifies the identification number of the crash record as an integer representing a valid record number from 1 through 120. To determine the numeric identity of a specific crash file, use the **show crash list** command in Exec mode.

url *to_url*

Specifies the destination of the copy. *url* may refer to a local or a remote file and must be entered using the following format:

- **[file:] { /flash | /pcmcia1 | /hd } [/***directory* **] /**
- **tftp://{** *host***[** *:port#* **] } [/***directory* **] /**
- **[ftp: | sftp:]//[** *username* **[** *:password* **] @] {** *host* **} [** *:port#* **] [/***directory* **] /**

Important: Use of the SMC hard drive is not supported in this release.

directory: the name of the target directory.
username: the username to be authenticated to provide access to targeted server.
password: the username's password to be authenticated.
host: the IP address or host name of the targeted server.
port#: the number of the target server's logical port used for the selected communication protocol.

Important: Do **not** specify a target filename as this will prevent the file from writing to the target server. The system generates and provides a timestamp-based filename that appears at the destination when the **copy** command completes.

core

Copies the core dump to the targeted storage server. The core cannot be copied alone; it must be part of a **crash copy** action included when copying a crash file.

Usage

Copy crash files of core dump to another location for backup or analysis.

Example

The following uses FTP to copy stored record number *5* and the core dump from the crash record list to a targeted remote node directory called *crasharchive* through port *22* of the targeted server *remoteABC* with access through user *homeboy* whose password is *secret.7.word*.

```
crash copy number 5 url ftp://homeboy:secret.7.word@
remoteABC:22/crasharchive/ core
```

crypto-group

Allows the manual switchover of redundant IPSec tunnels belonging to a specific crypto group.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

crypto-group name *group_name* **activate { primary | secondary }**

---

crypto-group name *group_name*

Specifies the name of an existing crypto group with which the tunnels to be switched are associated.

---

activate { primary | secondary }

Allows you to specify which tunnel to activate:

- **primary**: Switches traffic to the primary tunnel in the group.
- **secondary**: Switches traffic to the secondary tunnel in the group.

Usage

This command is used in conjunction with the Redundant IPSec Tunnel Fail-over feature.
Use this command to manually switch traffic to a specific tunnel in a crypto group if the automatic switchover options have been disabled. Refer to the **switchover** command in the Crypto Group configuration mode for more information.

Example

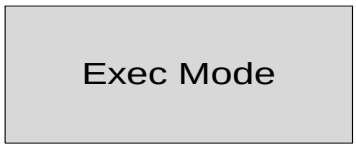
The following command manually switches user traffic to the secondary tunnel in the crypto group called *group1*:

```
crypto-group group1 activate secondary
```

Chapter 112
Exec Mode Commands (D-S)

This chapter contains the commands in the Exec Mode from **debug** to **system**.

The Exec Mode is the initial entry point into the command line interface system. Exec mode commands are useful in troubleshooting and basic system monitoring.



debug

The following commands send information to the logging facility for review:

- debug bfd
- debug ip
- debug ip bgp
- debug ip ospf all
- debug ip ospf event
- debug ip ospf ism
- debug ip ospf lsa
- debug ip ospf nsm
- debug ip ospf packet
- debug ip ospf route
- debug ip ospf router
- debug ipv6 ospf all (OSPFv3)
- debug ipv6 ospf event (OSPFv3)
- debug ipv6 ospf ifsm (OSPFv3)
- debug ipv6 ospf lsa (OSPFv3)
- debug ipv6 ospf nsm (OSPFv3)
- debug ipv6 ospf packet (OSPFv3)
- debug ipv6 ospf route (OSPFv3)

debug bfd

Enables or disables the debug options for Bidirectional Forwarding Detection BFD) debugging. If logging is enabled, results are sent to the logging system.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

`[ no ] debug bfd { all | events ipc-error | ipc-events | nsm | packet | session }`

`no`

Indicates the IP debugging is to be disabled for the IP interfaces/function specified.

`bfd | interface` *`name`* **`| route`**

Specifies which IP interfaces/function to debug.
`all`: enables debug for all BFD items.
`events`: enables debug for BFD events.
`ipc-error`: enables debug for BFD Inter-process communication (IPC) errors.
`ipc-events`: enables debug for BFD Inter-process communication (IPC) events.
`nsm`: enables debug for BFD Network Service Manager messages.
`packet`: enables debug for BFD packets.
`session`: enables debug for BFD sessions.

Usage

The debug bfd command is valuable when troubleshooting network problems with BFD-enabled BGP routers. The debugging is stopped by using the **`no`** keyword.

Caution: Issuing this command could negatively impact system performance depending on system configuration and/or loading.

Example

The following commands enable/disable debugging for BFD.

```
debug bfdno debug bfd
```

debug ip

Enables or disables the debug options for IP debugging. If logging is enabled, results are sent to the logging system.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ip { arp | interface | route }
```

no

Indicates the IP debugging is to be disabled for the IP interfaces/function specified.

arp | interface *name* **| route**

Specifies which IP interfaces/function to debug.
arp: indicates debug is to be enabled for the address resolution protocol.
interface: indicates debug is to be enabled for the IP interfaces.
route: indicates debug is to be enabled for the route selection and updates.

Usage

The debug IP command is valuable when troubleshooting network problems between nodes. The debugging is stopped by using the **no** keyword.

Caution: Issuing this command could negatively impact system performance depending on system configuration and/or loading.

Example

The following commands enable/disable debugging for ARP.

```
debug ip arpno debug ip arp
```

The following enables/disables debugging for IP interfaces.

```
debug ip interface
```

```
no debug ip interface
```

The following enables/disables debugging for routing.

```
debug ip routeno debug ip route
```

debug ip bgp

Enables or disables BGP (Border Gateway Protocol) debug flags. If logging is enabled, results are sent to the logging system.

Product

HA

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ip bgp { all | event | filters | fsm | keepalives | updates { inbound | outbound } }
```

no

Disables the specified BGP debug flags.

all

Enables all BGP debug flags.

event

Enables debugging of all BGP protocol events.

filters

Enables debugging of all BGP filters.

fsm

Enables debugging of BGP Finite State Machine

keepalives

Enables debugging of all BGP keepalives.

updates {inbound | outbound}

Enables debugging of BGP updates.
inbound: Debug all BGP inbound updates.
outbound: Debug all BGP outbound updates.

Usage

Use this command to enable or disable BGP debug flags.

Example

The following command disables all BGP debug flags enabled by any of the **debug ip bgp** commands:

```
no debug ip bgp all
```

The following command enables all BGP debug flags:

```
debug ip bgp all
```

debug ip ospf all

Enables or disables all OSPF (Open Shortest Path First) debug flags. If logging is enabled, results are sent to the logging system.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

`[ no ] debug ip ospf all`

`no`

Disable all OSPF debug flags.

Usage

Use this command to enable or disable all OSPF debug flags.

Example

The following command disables all OPSF debug flags enabled by any of the **`debug ip ospf`** commands:

```
no debug ip ospf all
```

The following command enables all OSPF debug flags:

```
debug ip ospf all
```

debug ip ospf event

Enables or disables debugging of OSPF protocol events. If logging is enabled, results are sent to the logging system. If no keywords are specified, all events are enabled for debugging.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ip ospf event [ abr | asbr | vl | lsa | os | router ]
```

no

Disables debugging the specified OSPF event. If no keywords are specified, all events are disabled.

abr

Enables debugging of Area Border Router (ABR) events.

asbr

Enables debugging of Autonomous System Boundary Router (ASBR) events.

vl

Enables debugging of Virtual Link (VL) events.

lsa

Enables debugging of link state advertisement (LSA) events.

os

Enables debugging of operating system (OS) events.

router

Enables debugging of router events.

Usage

Use this command to output debug information for OSPF events.

Example

To enable all event debug information, enter the following command;

```
debug ip ospf event
```

To disable all event debug information, enter the following command;

```
no debug ip ospf event
```

debug ip ospf ism

Enables or disables OSPF Interface State Machine (ISM) troubleshooting, based on ISM information type. If no keywords are specified all ISM information types are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ip ospf ism [ events | status | timers ]
```

no

Disables debugging the specified ISM information. If no keywords are specified, all information is disabled.

events

Enables debugging ISM event information.

status

Enables debugging ISM status information.

timers

Enables debugging ISM timer information.

Usage

Use this command to output ISM debug information.

Example

To enable all ISM debug information, enter the following command;

```
debug ip ospf ism
```

To disable all ISM debug information, enter the following command;

```
no debug ip ospf ism
```

debug ip ospf lsa

Enables or disables troubleshooting on OSPF Link State Advertisements (LSAs), based on the specific LSA option. If no keywords are specified, all options are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ip ospf lsa [ flooding | generate | install | refresh | maxage | refresh ]
```

no

Disables the specified LSA debug information. If no keyword is specified, all LSA debug information is disabled.

flooding

Enables LSA flooding information.

generate

Enables LSA generation information.

install

Enables LSA install information.

maxage

Enables LSA maximum age information in seconds. The maximum age is 3600 seconds.

refresh

Enables LSA refresh information.

Usage

Use this command to output debug information for LSAs.

Example

To enable all LSA debug information, enter the following command;

```
debug ip ospf lsa
```

To disable all LSA debug information, enter the following command;

```
no debug ip ospf lsa
```

debug ip ospf nsm

Enables or disables troubleshooting OSPF Neighbor State Machines (NSMs), based on the specific NSM information type. If no keyword is specified, all NSM information types are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ip ospf nsm [ status | events | timers ]
```

no

Disables the debugging the specified NSM information type. If no keyword is specified, all information types are disabled.

events

Enables debugging NSM event information.

status

Enables debugging NSM status information.

timers

Enables debugging NSM timer information.

Usage

Use this command to output debug information for OSPF NSMs

Example

To enable all NSM debug information, enter the following command;

```
debug ip ospf nsm
```

To disable all NSM debug information, enter the following command;

```
no debug ip ospf nsm
```

debug ip ospf packet

Enables or disables troubleshooting of specific OSPF packet information. If logging is enabled, results are sent to the logging system.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ip ospf packet { all | dd | hello | ls-ack | ls-request | ls-update } [ send
| recv ] [ detail ]
```

no

Disable debugging of the specified packet information.

all

Enables debugging all OSPF packet information.

dd

Enables debugging database descriptions.

hello

Enables debugging hello packets.

ls-ack

Enables debugging link state acknowledgements.

ls-request

Enables debugging link state requests.

ls-update

Enables debugging link state updates.

send

Enables debugging only on sent packets.

recv

Enables debugging only on received packets.

detail

Enables detailed information in the debug output.

Usage

Use this command to output specific OSPF packet information.

Example

To enable all packet debug information, enter the following command;

```
debug ip ospf packet all
```

To disable all route debug information, enter the following command;

```
no debug ip ospf packet all
```

debug ip ospf route

Sets the route calculation method to use in debugging OSPF routes. If no route calculation method is specified, all methods are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ip ospf route [ ase | ia | install | spf ]
```

no

Disables debugging of route information. If no keyword is specified all information types are disabled.

ase

Enables debugging information on autonomous system external (ASE) route calculations.

ia

Enables debugging information on Inter-Area route calculations.

install

Enables debugging information on route installation.

spf

Enables debugging information on Shortest Path First (SPF) route calculations.

Usage

Use this command to output debug information for OSPF routes.

Example

To enable all route debug information, enter the following command;

```
debug ip ospf route
```

To disable all route debug information, enter the following command;

```
no debug ip ospf route
```

debug ip ospf router

Sets the debug option for OSPF router information. If no keyword is specified, all router information is enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ip ospf router [ interface | redistribute ]
```

no

Disables the specified router debug information. If no keyword is specified, all router information is disabled.

interface

Enables router interface information.

redistribute

Enables router redistribute information.

Usage

Use this command to output debug information for the OSPF router.

Example

To enable all router debug information, enter the following command;

```
debug ip ospf router
```

To disable all router debug information, enter the following command;

```
no debug ip ospf router
```

debug ipv6 ospf all

Enables or disables all OSPFv3 (Open Shortest Path First Version 3) debug flags. If logging is enabled, results are sent to the logging system.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ipv6 ospf all
```

no

Disable all OSPFv3 debug flags.

Usage

Use this command to enable or disable all OSPFv3 debug flags.

Example

The following command disables all OPSFv3 debug flags enabled by any of the **debug ip ospf** commands:

```
no debug ipv6 ospf all
```

The following command enables all OSPFv3 debug flags:

```
debug ipv6 ospf all
```

debug ipv6 ospf event

Enables or disables debugging of OSPFv3 protocol events. If logging is enabled, results are sent to the logging system. If no keywords are specified, all events are enabled for debugging.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ipv6 ospf event [ abr | asbr | os | router ]
```

no

Disables debugging the specified OSPFv3 event. If no keywords are specified, all events are disabled.

abr

Enables debugging of Area Border Router (ABR) events.

asbr

Enables debugging of Autonomous System BOundary Router (ASBR) events.

os

Enables debugging of operating system (OS) events.

router

Enables debugging of router events.

Usage

Use this command to output debug information for OSPFv3 events.

Example

To enable all event debug information, enter the following command;

```
debug ipv6 ospf event
```

To disable all event debug information, enter the following command;

```
no debug ipv6 ospf event
```

debug ipv6 ospf ifsm

Enables or disables OSPFv3 Interface State Machine (ISM) troubleshooting, based on ISM information type. If no keywords are specified all ISM information types are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ipv6 ospf ism [ events | status | timers ]
```

no

Disables debugging the specified ISM information. If no keywords are specified, all information is disabled.

events

Enables debugging ISM event information.

status

Enables debugging ISM status information.

timers

Enables debugging ISM timer information.

Usage

Use this command to output ISM debug information.

Example

To enable all ISM debug information, enter the following command;

```
debug ipv6 ospf ism
```

To disable all ISM debug information, enter the following command;

```
no debug ipv6 ospf ism
```

debug ipv6 ospf lsa

Enables or disables troubleshooting on OSPFv3 Link State Advertisements (LSAs), based on the specific LSA option. If no keywords are specified, all options are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ip ospf lsa [ flooding | generate | install | maxage | refresh ]
```

no

Disables the specified LSA debug information. If no keyword is specified, all LSA debug information is disabled.

flooding

Enables LSA flooding information.

generate

Enables LSA generation information.

install

Enables LSA install information.

maxage

Enables LSA maximum age information in seconds. The maximum age is 3600 seconds.

refresh

Enables LSA refresh information.

Usage

Use this command to output debug information for LSAs.

Example

To enable all LSA debug information, enter the following command;

```
debug ipv6 ospf lsa
```

To disable all LSA debug information, enter the following command;

```
no debug ipv6 ospf lsa
```

debug ipv6 ospf nsm

Enables or disables troubleshooting OSPFv3 Neighbor State Machines (NSMs), based on the specific NSM information type. If no keyword is specified, all NSM information types are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ipv6 ospf nsm [ interface | redistribute ]
```

no

Disables the debugging the specified NSM information type. If no keyword is specified, all information types are disabled.

interface

Enables debugging NSM on this interface.

redistribute

Enables debugging NSM redistribution information.

Usage

Use this command to output debug information for OSPFv3 NSMs

Example

To enable all NSM debug information, enter the following command;

```
debug ipv6 ospf nsm
```

To disable all NSM debug information, enter the following command;

```
no debug ipv6 ospf nsm
```

debug ipv6 ospf packet

Enables or disables troubleshooting of specific OSPFv3 packet information. If logging is enabled, results are sent to the logging system.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ipv6 ospf packet { dd | hello | ls-ack | ls-request | ls-update } [ recv | send ] [ detail ]
```

no

Disable debugging of the specified packet information.

dd

Enables debugging database descriptions.

hello

Enables debugging hello packets.

ls-ack

Enables debugging link state acknowledgements.

ls-request

Enables debugging link state requests.

ls-update

Enables debugging link state updates.

recv

Enables debugging only on received packets.

send

Enables debugging only on sent packets.

detail

Enables detailed information in the debug output.

Usage

Use this command to output specific OSPFv3 packet information.

Example

To enable all packet debug information, enter the following command;

```
debug ipv6 ospf packet all
```

To disable all route debug information, enter the following command;

```
no debug ipv6 ospf packet all
```

debug ipv6 ospf route

Sets the route calculation method to use in debugging OSPFv3 routes. If no route calculation method is specified, all methods are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] debug ipv6 ospf route [ ase | ia | install | spf ]
```

no

Disables debugging of route information. If no keyword is specified all information types are disabled.

ase

Enables debugging information on autonomous system external (ASE) route calculations.

ia

Enables debugging information on Inter-Area route calculations.

install

Enables debugging information on route installation.

spf

Enables debugging information on Shortest Path First (SPF) route calculations.

Usage

Use this command to output debug information for OSPF routes.

Example

To enable all route debug information, enter the following command;

```
debug ipv6 ospf route
```

To disable all route debug information, enter the following command;

```
no debug ipv6 ospf route
```

default terminal

Restores the system default value for the terminal options.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
default terminal { length | width }
```

length | width

length: Resets the terminal length to the system default.
width: Resets the system default terminal width.

Usage

Restore the default terminal settings when the current paging and display wraps inappropriately or pages to soon.

Example

The following sets the default length then width in two commands.

```
default terminal length

default terminal width
```

delete

Removes the specified file(s) permanently from the local.

Product

All

Privilege

Security Administrator, Administrator

Syntax

delete *filepath* **[-noconfirm]**

filepath

Specifies the location of the file to rename. The path must be formatted as follows:
[**file:**]{ **/flash** | **/pcmcia1** | **/hd** }[**/***directory*]**/***file_name*

Important: Use of the SMC hard drive is not supported in this release.

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name
filename is the actual file of interest

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Important: Use of the **-noconfirm** option should be done with extra care to ensure the file is specified accurately as there is no method of recovering a file that has been deleted.

Usage

Deleting files is a maintenance activity which may be part of periodic routine procedures to reduce system space utilization.

Example

The following removes files from the local */flash/pub* directory.

```
delete /flash/pub/june03.cfg
```

dhcp force

Tests the lease-renewal for DHCP-assigned IP addresses for a particular subscriber.

Product

GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator

Syntax

dhcp force lease-renewal { **callid** *id* | **imsi** *imsi* [**nsapi** *nsapi*] | **msid** *msid* }

callid *id*

Clears the call ID specified as a 4-byte hexadecimal number.

imsi *msid*

Disconnects the subscriber with the specified msid. The IMSI (International Mobile Subscriber Identity) ID is a 50-bit field which identifies the subscriber's home country and carrier. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘). For example; ‘$’.

nsapi *nsapi*

Specifies a Network Service Access Point Identifier (NSAPI) an integer from 5 to 15.

msid *id*

Disconnects the mobile user identified by *ms_id*. *ms_id* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘). For example; ‘$’.

Usage

Use this command tests a forced IP address lease renewal for a specific subscriber.

Example

The following command tests DHCP lease renewal for a subscriber with an MSID of *1234567*:

```
dhcp force lease-renewal msid 1234567
```

dhcp test

Tests DHCP (Dynamic Host Configuration Protocol) functions for a particular DHCP service.

Product

GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator

Syntax

dhcp test dhcp-service *svc_name* [**all** | **server** *ip_address*]

dhcp-service *svc_name*

Specifies the name of the DHCP service as an alphanumeric string of 1 through 63 characters that is case sensitive.

all

Tests DHCP functionality for all servers.

server *ip_address*

Tests DHCP functionality for the server specified by an IP address entered using IPv4 dotted-decimal notation.

Usage

Once DHCP functionality is configured on the system, this command can be used to verify that it is configured properly and that it can successfully communicate with the DHCP server.
Executing this command causes the system to request and allocate an IP address and then release it.
If a specific DHCP server is not specified, then each server configured in the service is tested.

Example

The following command tests the systems ability to get an IP address from all servers a DHCP service called *DHCP-Gi* is configured to communicate with:

```
dhcp test dhcp-service DHCP-Gi all
```

diameter disable endpoint

Disables a Diameter endpoint without removing the peer's configuration.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter disable endpoint *endpoint_name* **peer** *peer_id*

endpoint *endpoint_name*

Specifies the endpoint in which the peer is configured as an alphanumeric string of 1 through 63 characters.

peer *peer_id*

Specifies the Diameter peer host name to be disabled as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to administratively disable a Diameter peer without removing the peer configuration. This command will tear down all connections on the specified peer (by sending a DPR if the configuration demands the same at peer level configuration). The peer will remain in disabled state until it is enabled again. Also see the **diameter enable endpoint** command.

Example

This command disables the Diameter peer *peer12*:

```
diameter disable endpoint endpoint1 peer peer12
```

diameter enable endpoint

Enables a Diameter endpoint that is disabled.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter enable endpoint *endpoint_name* **peer** *peer_id*

endpoint *endpoint_name*

Specifies the endpoint in which the peer is configured as an alphanumeric string of 1 through 63 characters.

peer *peer_id*

Specifies the Diameter peer host name to be enabled as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to administratively enable a Diameter peer. Also see the **diameter disable endpoint** command.

Example

This command enables the Diameter peer *peer12*:

```
diameter enable endpoint endpoint1 peer peer12
```

diameter reset connection

Resets individual TCP/SCTP connections for a specified Diameter endpoint.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

diameter reset connection { endpoint *endpoint_name* **peer** *peer_id* **}**

endpoint *endpoint_name*

Resets connection to the endpoint specified as an alphanumeric string of 1 through 63 characters.

peer *peer_id*

Resets connection to the Diameter peer host name specified as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to reset the TCP/SCTP connections for the specified endpoint/peer. With this command, the connection will be closed temporarily after DPR/DPA. If there is any traffic to be sent to the particular peer, then the connection will be re-established.
This command overrides the endpoint configured in any other configuration mode.
This command is applicable only when the specified peer is enabled.

Example

This command resets connection to the endpoint named *test123*:

```
diameter reset connection endpoint test123
```

diameter reset route failure

Resets the failed route status of a Diameter destination-host combination via peer to AVAILABLE status.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

diameter reset route failure [endpoint *endpoint_name* **] [host** *host_name* **] [peer** *peer_id* **]**

endpoint *endpoint_name*

Resets paths to the endpoint specified as an alphanumeric string of 1 through 63 characters.

host *host_name*

Resets the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis having a specific host name to AVAILABLE.
Specifies the Diameter host name as an alphanumeric string of 1 through 63 characters.

peer *peer_id*

Resets the FAILED status of all Diameter destination-host combination routes via a peer having specific peer-Id for every Diameter client within the chassis to AVAILABLE.
Specifies the Diameter peer host name as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to reset the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis to AVAILABLE status.
This command also resets the failure counts used to determine the AVAILABLE/FAILED status of a destination-host combination.
When executed from local context, this command matches all contexts. If an optional keyword is not supplied, a wildcard is used for the value.
The status of every matching combination of destination-host via peer for every matching Diameter client within the chassis will be reset to AVAILABLE. The failure counts that are used to determine AVAILABLE/FAILED status will also be reset.
Also see the **route-entry** and **route-failure** commands in the *Diameter Endpoint Configuration Mode Commands* chapter.
Default value: N/A

Example

The following command resets the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis for specified endpoint name to AVAILABLE.

```
diameter reset route failure endpoint endpoint123
```

directory

Lists the files in a specified location.

Product

All

Privilege

Security Administrator, Administrator

Syntax

directory *filepath* **[-size] [-reverse] [-time]**

filepath

Specifies the directory path to list the contained files using the following format:
[**file:**]{ **/flash** | **/pcmcia1** | **/hd** }[**/***directory*]**/***file_name*

Important: Use of the SMC hard drive is not supported in this release.

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name
filename is the actual file of interest

-size

Indicates the size of each file should be displayed in the output.

-reverse

Indicates the order of files listed should be in descending order (z-aZ-A9-0). Default is to sort in ascending order (0-9A-Za-z).

-time

Indicates the last modification timestamp of each file should be displayed in the output.

Usage

Lists such things as log and crash files from multiple nodes within the network.
The optional arguments may be specified individually or in any combination.

Example

The following command will list the files in the local */flash/pub* directory sorted in reverse order.

```
directory /flash/pub -reverse
```

disable radius

Prevents the system from making requests of a selected RADIUS server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

disable radius { [charging] [accounting] server *ipv4/ipv6_address* **[group** *group_name* **| port** *port_number* **+] }**

[charging] [accounting]

Specifies the type of RADIUS server to disable.

- **accounting**: Specifies accounting servers
- **charging**: Specifies charging servers
- **charging accounting**: Specifies charging accounting servers

server *ipv4/ipv6_address*

Specifies the RADIUS server by IP address entered using IPv4 dotted-decimal or IPv6 colon-separated notation.

port *port_number*

Specifies the port number of the RADIUS server being disabled an integer from 0 through 65535. Default: 1812 (authentication) 1813 (accounting)

group *group_name*

Specifies the RADIUS group to which the server belongs as an alphanumeric string of 1 through 63 characters. Use this option in the event that the RADIUS server belongs to multiple groups and you only want to disable the server within the specific group. Default: **default**

Usage

Use this command to gracefully stop the system from making requests of a specific RADIUS server.

Example

The following command disables a RADIUS accounting server with an IP address of *10.2.3.4*, the default accounting server port number, and that resides in the *Group5* server group:

```
disable radius accounting server 10.2.3.4 group Group5
```

dns-client

Performs DNS (Domain Name System) query on the basis of specified DNS client name, DNS query domain name, and type of query criteria.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

dns-client *dns_client_name* **[query-type { A | AAAA | NAPTR | SRV }] query-name** *query_domain_name*

dns-client *dns_client_name*

Specifies the name of the DNS client whose cache and/or statistics are to be queried. It must be an existing DNS client expressed as an alphanumeric string of 1 through 64 characters.

query-type { A | NAPTR | SRV }]

Specifies that the type of query to perform for the defined DNS client is to be displayed.

- **A**: Filters DNS results based on domain IPv4 address records (A records). This is the default query type.
- **AAAA**: Filters DNS results based on domain IPv6 address records (AAAA records).
- **NAPTR**: Filters DNS results based on Naming Authority Pointer records (NAPTR).
- **SRV**: Filters DNS results based on service host records (SRV records).

query-name *query_domain_name*

Filters the DNS results based on the query domain name expressed as an alphanumeric string of 1 trough 255 characters.
query_domain_name is the domain name used to perform the DNS query and is different from the actual domain name which is resolved. For example, to resolve the SIP server for *service.com*, the query name is *_sip._udp.service.com* and the query type is **SRV**.

Usage

Use this command to perform DNS query on the basis of DNS Client name and filters the query results based on query type and query name. This command also populates the result into DNS Cache. This command used the current context to DNS request.

Example

The following command displays statistics for a DNS client named *test_dns* with query type for IP address as *A* and query name as *domain1.com*:

```
dns-client test_dns query-type A query-name domain1.com
```

enable radius

Enables the system to start making requests of a specific RADIUS server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

enable radius { [charging] [accounting] server *ipv4/ipv6_address* **[group** *group_name* **| port** *port_number* **+] }**

[charging] [accounting]

Specifies the type of RADIUS server to enable.

- **accounting**: Specifies accounting servers
- **charging**: Specifies charging servers
- **charging accounting**: Specifies charging accounting servers

server *ipv4/ipv6_address*

Specifies the RADIUS server by an IP address entered using IPv4 dotted-decimal or IPv6 colon-separated notation.

port *port_number*

Specifies the port number of the RADIUS server being enabled as an integer from 0 through 65535. Default: 1812 (authentication) 1813 (accounting)

group *group_name*

Specifies the RADIUS group to which the server belongs as an alphanumeric string of 1 through 63 characters. Use this option in the event that the RADIUS server belongs to multiple groups and you only want to disable the server within the specific group. Default: **default**

Usage

Use this command to allow the system to start making requests of a specific RADIUS server.

Example

The following command enables a RADIUS accounting server with the IP address *10.2.3.4*, the default accounting server port number, and in the *Group5* server group:

```
enable radius accounting server 10.2.3.4 group Group5
```

exit

Terminates the current CLI session.

Product

All

Privilege

Any

Syntax

```
exit
```

Usage

Use this command to terminate the current CLI session.

filesystem

Use this command to check, format or repair the filesystem on internal and external storage devices.

Product

All

Privilege

Security Administrator, Administrator

Syntax

filesystem { check | format | repair } { /flash | /pcmcia1 | /hd-raid } [card *card_num* **]**

filesystem { check | format | repair } { /flash | /usb1 | /hd-raid } [card *card_num* **]**

Usage

Check, format, or repair all directories and files from on an internal or external storage device and re-establish the file system.

Example

The following command formats the PCMCIA card located in slot 1 on the SMC:

```
filesystem format /pcmcia1
```

filesystem synchronize

Use this command to manage the Switch Processor Cards (SPCs) or System Management Cards (SMCs) and their active/standby status, and to synchronize the filesystem between the active device and the standby device.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

filesystem synchronize [/flash | /pcmcia1 | all] [checkonly] [from *card_num* **| to** *card_num* **] [-noconfirm]**

Usage

Synchronize the file system between the active device and the standby device.

gtpc test echo

Tests the ability of a GGSN service to exchange GTP-C echo request messages with the specified SGSN(s).

Product

GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

gtpc test echo src-address *gn_address* { **all** | **sgsn-address** *ip_address* }

src-address *gn_address*

Specifies the IP address of a Gn interface configured on the system in IPv4 dotted-decimal notation.

Important: The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.

all

Specifies that GTP-C echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.

sgsn-address *ip_address*

Specifies that GTP-C echo requests will be sent to a SGSN specified by an IP address in IPv4 dotted-decimal notation.

Usage

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol control plane (GTP-C) packets with the specified SGSNs. This command is useful for troubleshooting and/or monitoring. This command must be executed from within the context in which the GGSN service is configured. Refer also to the **gtpu test** command.

Example

The following command issues GTP-C echo packets from a GGSN service bound to address *192.168.157.32* to an SGSN with an address of *192.168.157.2*:

```
gtpc test echo src-address 192.168.157.32 sgsn-address 192.168.157.2
```

gtpp interim now

Check points current GTPP accounting messages and identifies which types of interim CDRs are to be generated and sent to the external charging/storage servers (for example, a CFG or a GSS). The impact of this command is immediate.

Product

GGSN, SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

gtpp interim now [**active-charging egcdr** | **apn** *apn_name* | **callid** *call_id* | **cdr-types** { **gcdr** | **mcdr** | **scdr** } | **dhcp-server** *ip_address* | **gprs-service** *svc_name*| **ggsn-address** *ggsn_ip_addr* | **ggsn-service** *svc_name* | **imsi** *imsi* [**ip-address** *sub_address* [**username** *name*] **now** | **nsapi** *nsapi* [**ip-address** *sub-address* [**username** *name*] | **username** *name*]] | **ip-address** *sub_address* [**username** *name*] | **ip-pool** *pool_name* | **mcc** *mcc_number* **mnc** *mnc_number* | **msisdn** *msisdn_num* | **sgsn-address** *ip_address* | **sgsn-service** *svc_name* | **username** *name*] +

active-charging

This feature is specific to the GGSN and is documented separately. .

apn *apn_name*

Initiates GTPP interim accounting for all PDP contexts accessing the APN specified as an alphanumeric string of 1 through 62 characters that is case sensitive.

callid *call_id*

Identifies a specific call id as an 8-digit hexadecimal number.

cdr-types { mcdr | scdr }

Specifies the CDR types to be generated by the SGSN:
gcdr - Instructs the GGSN to only generate G-CDRs.
mcdr - Instructs the SGSN to only generate M-CDRs
scdr - Instructs the SGSN to only generate S-CDRs.
This keyword is specific to the SGSN.

dhcp-server *ip_address*

Identifies the DHCP server where the IP address (defined with the **ip address** keyword) was allocated by the IP address of the DHCP server entered using IPv4 dotted-decimal notation.

ggsn-address *ggsn_ip_addr*

Specifies the IP address of the interface to the GGSN using IPv4 dotted-decimal notation. This keyword is specific to the GGSN.

ggsn-service *svc_name*

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by the GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive. This keyword is specific to the GGSN.

gprs-service *svc_name*

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by an existing GPRS service specified as an alphanumeric string of 1 through 63 characters that is case sensitive. This keyword is specific to the SGSN.

imsi *imsi* **[ip-address** *sub_address* **[username** *name* **] | nsapi** *nsapi* **[ip-address** *sub-address* **[username** *name* **] | username** *name* **]]**

Initiates GTPP interim accounting for a specific International Mobile Subscriber Identity (IMSI) number. The request could be further filtered using any of the following keywords:

- **ip-address**: Interim accounting will be performed for the IP address specified by *sub_address*. The command can be further filtered by specifying a specific username with that address.
- **nsapi**: Interim accounting will be performed for a Network Service Access Point Identifier (NSAPI) specified as an integer from 5 to 15. The command can be further filtered by specifying a specific ip address and/or a username with that address, or just a specific username.

ip-address *sub_address* **[username** *name* **]**

Initiates GTPP interim accounting for the IP address of the subscriber specified in IPv4 dotted-decimal notation.
The command can be further filtered by specifying a username with that address. The name is the subscriber's name and can be a sequence of characters and/or wildcard characters ('$' and '*') from 1 to 127 characters. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes (‘). For example; ‘$’.

ip-pool *pool_name*

Initiates GTPP interim accounting for all PDP contexts that were allocated IP addresses from an existing pool specified as an alphanumeric string of 1 through 31 characters that is case sensitive. This keyword is applicable to the GGSN only.

mcc *mcc_number* **mnc** *mnc_number*

mcc_number: Specifies the mobile country code (MCC) portion of the PLMN identifier and can be configured to any 3-digit integer value between 100 and 999.
mnc_number: Specifies the mobile network code (MNC) portion of the PLMN identifier and can be configured to any 2- or 3-digit integer between 00 and 999.

msisdn *msisdn_num*

Configures the SGSN to include the Mobile Subscribers Integrated Services Digital Network identifier in generated CDRs (M-CDRs and/or the S-CDRs). This keyword is applicable for SGSN only.
msisdn_number must be followed by a valid MSISDN number, consisting of 1 to 15 digits.

sgsn-address *ip_address*

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by the SGSN specified by an IP address in IPv4 dotted-decimal notation. This keyword is specific to the GGSN.

sgsn-service *svc_name*

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by an existing SGSN service specified an alphanumeric string of 1 through 63 characters that is case sensitive. This keyword is specific to the SGSN.

username *name*

Initiates GTPP interim accounting for all PDP contexts for the subscriber name specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

+

More than one of the above keywords can be entered within a single command.

Usage

This command causes GTPP accounting CDRs to immediately be generated for all active sessions that are in the current context. If executed within the local context, CDRs will be generated for all active sessions regardless of context.
The sending of the CDRs is paced so as not to overload the accounting server.

Example

The following command causes CDRs to immediately be generated:

```
gtpp interim now
```

gtpp interim now active-charging egcdr

Check points current GTPP accounting messages for active charging immediately.

Product

GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
gtpp interim now active-charging egcdr [ callid call_id | imsi imsi | msid msid |
rulebase rbase_name | session-id sess_id | username name ]
```

callid *call_id*

Initiates GTPP interim accounting for a session for the call ID specified as an 8-digit hexadecimal number.

imsi *imsi*

Initiates GTPP interim accounting for a International Mobile Subscriber Identity (IMSI) number. specified as a sequence of hexadecimal digits and wildcard characters - $ matches a single character and * matches multiple characters

msid *msid*

Initiates GTPP interim accounting for a Mobile Station Identifier (MSID) number specified as a sequence of up to 24 digits and wildcard characters - $ matches a single character and * matches multiple characters

rulebase *rbase_name*

Initiates GTPP interim accounting for sessions that use the named active charging rulebase specified as an alphanumeric string of 1 through 24 characters.

session-id *sess_id*

Initiates GTPP interim accounting for a current active charging session.

username *name*

Initiates GTPP interim accounting for all PDP contexts for the subscriber name specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

Usage

This command causes GTPP accounting eG-CDRs to immediately be generated for active charging sessions that meet the specified criteria.
The sending of the CDRs is paced so as not to overload the accounting server.

Example

The following command causes eG-CDRs to immediately be generated for active charging sessions using the rulebase named rulbase1:

```
gtpp interim now active-charging egcdr rulebase rulebase1
```

gtpp storage-server commit

Causes the GTPP storage server to archive all buffered packets.

Product

GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

```
gtpp storage-server commit now [ group name group_name ]
```

group name *group_name*

Commits Storage Server for an existing group name expressed as an alphanumeric string of 1 through 63 characters.

Usage

This command sends a request to the GTPP Storage Server to archive all buffered packets. It also deletes all CDRs that have been acknowledged by the charging gateway function (CGF). The deleted CDRs are saved in a separate file.

Note that this command must be executed from within the context in which the GTPP Storage Server is configured.

Refer to the **gtpp storage-server** command in the *Context Configuration Mode Commands* chapter for more information.

gtpp test

Tests communication with configured charging gateway function (CGF) severs or a GTPP Storage-Server.

Product

GGSN

Privilege

Operator, Config-Administrator, Administrator

Syntax

```
gtpp test { accounting { all | cgf-server cgf_address | group name group_name } |
storage-server [ address ip-addr port udp-port |  group name group_name ] }
```

all

Tests all CGFs configured within the given context.

cgf-server *cgf_address*

Tests a CGF configured within the given context and specified by the IP address of the CGF entered using IPv4 dotted-decimal notation.

group name *group_name*

Tests the storage server for an existing group name specified as an alphanumeric string of 1 through 63 characters.

storage-server [address *ip-address* **port** *udp-port*]

Tests the connectivity and provides round trip time for the echo request sent to the GTPP Storage-Server configured in the requested context. The IP address of the GSS is entered using IPv4 dotted-decimal notation and the UPD port is the one defined for the GTPP Storage Server.

Usage

This command is used to verify the configuration of and test the system's ability to communicate with one or all configured GSS/CGFs for monitoring or troubleshooting purposes.
When executed, this command causes the system to send GTPP echo packets to the specified GSS/CGF(s). The command's response will display whether the GSS/CGF is active or unreachable.

Example

The following command tests communication with a CGF having an IP address of *192.168.1.5*:

```
gtpp test accounting cgf-server 192.168.1.5
```

The following command tests communication with a GSS configured in requested context

```
gtpp test storage-server
```

The following command verify communication with a GSS, having IP address *192.156.12.10* and port *50000*, without configuring it in a context

```
gtpp test storage-server address 192.156.12.10 port 50000
```

gtpu test echo

Tests the ability of a GGSN service to exchange GTP-U echo request messages with the specified SGSN(s).

Product

GGSN

Privilege

Operator, Config-Administrator, Administrator

Syntax

gtpu test echo src-address *gn_address* { **all** | **sgsn-address** *ip_address* }

src-address *gn_address*

Specifies the IP address of a Gn interface configured on the system using IPv4 dotted-decimal notation.

Important: The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.

all

Sends GTP-U echo requests to all SGSNs that currently have sessions with the GGSN service.

sgsn-address *ip_address*

Sends GTP-U echo requests to an SGSN specified by its IP address in IPv4 dotted-decimal notation.

Usage

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol user plane (GTP-U) packets with the specified SGSNs. This command is useful for troubleshooting and/or monitoring.
This command must be executed from within the context in which the GGSN service is configured.
Refer also to the **gtpc test** command.

Example

The following command issues GTP-U echo packets from a GGSN service bound to address *192.168.157.43* to an SGSN with an address of *192.168.1.52*:

```
gtpu test echo src-address 192.168.157.43 sgsn-address 192.168.1.52
```

gtpv0 test echo

Tests the ability of a GGSN service to exchange GTPv0 echo request messages with the specified SGSN(s).

Product

GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

gtpv0 test echo src-address *gn_address* { **all** | **sgsn-address** *ip_address* }

src-address *gn_address*

Specifies the IP address of a Gn interface configured on the system using IPv4 dotted-decimal notation.

Important: The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.

all

Sends GTPv0 echo requests to all SGSNs that currently have sessions with the GGSN service.

sgsn-address *ip_address*

Sends GTPv0 echo requests to an SGSN specified by its IP address in IPv4 dotted-decimal notation.

Usage

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol version 0 (GTPv0) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring.
This command must be executed from within the context in which the GGSN service is configured.
Refer also to the gtpc test and gtpu test commands.

Example

The following command issues GTPv0 echo packets from a GGSN service bound to address *192.168.1.33* to an SGSN with an address of *192.168.1.42*:

```
gtpv0 test echo src-address 192.168.1.33 sgsn-address 192.168.1.42
```

hd raid

Performs RAID management operations on the hard drives of redundant SMCs.

Product

All

Privilege

Security Administrator, Administrator

Syntax

hd raid { check | create { *local1* **|** *remote1* **} | overwrite {** *local1* **|** *remote1* **} | select {** *local1* **|** *remote1* **} | insert {** *local1* **|** *remote1* **} | { remove {** *local1* **|** *remote1* **} } [-force] [-noconfirm]**

check

Starts a background check on RAID disks unless the RAID is running in degraded mode.

create *local1* **|** *remote1*

Creates a new RAID that could run in degraded mode on the specified drive:
local1 specifies the RAID is to be established on the primary SMC. *remote1* specifies the RAID is to be established on the backup SMC.

overwrite *local1* **|** *remote1*

Overwrites the specified disk and adds it to the current running RAID to construct a fully mirrored array.
local1 specifies the primary SMC is to be added to the current RAID. *remote1* specifies the backup SMC is to be added to the current RAID.

select *local1* **|** *remote1*

Selects the specified disk to assemble a RAID when two unrelated RAID disks are present in the system. The resulting RAID runs in degraded mode.
local1: specifies the primary SMC is to assemble the RAID. *remote1:* specifies the backup SMC is to assemble the RAID.

insert *local1* **|** *remote1*

Inserts the specified disk to the running RAID causing it to recover from degraded mode.
local1: specifies the primary SMC is to be inserted into the RAID. *remote1:* specifies the backup SMC is to be inserted into the RAID.

remove local1 | remote1

Removes the specified disk from the running RAID causing it to run in degraded mode or to fail.
local1: specifies the primary SMC is to be removed from the RAID. *remote1:* specifies the backup SMC is to be removed from the RAID.

-noconfirm

Executes the command without displaying “are you sure” prompts.

-force

Executes the command and overrides warnings.

Usage

All commands need confirmation unless the **-noconfirm** is included in the command. If the result will bring down a running RAID, you have to force the command using **-force**.
RAID commands are needed to intervene in the following situations:

- the hard disk controller task can not determine the correct operation,
- administrator action is required by policy
- the administrator wants to wipe out an unused disk.

In an automated system, the policies created with this CLI address the possibility of a manually partitioned disk, a disk resulting from a different version of software, a partially constructed disk, or the case of two unrelated disks in the system.
To reduce administrator intervention, a set of policies can be configured to set the default action using the commands in the HD RAID configuration mode. These **hd raid** commands are described in the *HD RAID Configuration Mode* chapter of this guide.

Example

The following instructs the system to setup a RAID on the primary SMC hard drive.

```
hd raid create local1 -force
```

host

Used to resolve the IP address or logical host name information via a DNS query.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

host { *host_name* | *host_ip_address* }

host_name | *host_ip_address*

Specifies the host for which IP information is to be displayed.
host_name: Specifies the logical host name for which the IP address is to be displayed (via DNS lookup). This is an alphanumeric string of 1 through 127 characters.
host_ip_address: Specifies the IP address for which the associated logical host name(s) are to be displayed (via reverse DNS lookup) using IPv4 dotted-decimal notation.

Usage

Verify DNS information which affects connections and packet routing.

Example

The following commands will resolve the host information for *remoteABC* and *10.2.3.4* respectively.

```
host remoteABC

host 10.2.3.4
```

interface

Configures the system to generate gratuitous ARP (G-ARP) requests in case of a failure during an inter-node online upgrade. If the chassis is not active, an error message displays.

Product

All

Privilege

Security Administrator, Administrator, Operator, or Inspector with li-administrator permissions

Syntax

interface *name* **send gratuitous-arp** *ip-address*

Usage

This command generates a G-ARP for the IP address specified and sends it over the interface.

Example

The following generate a G-ARP for IP address *192.168.100.10*.

```
interface interface_1 send gratuitous-arp 192.168.100.10
```

lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

lawful-intercept packet-cable

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

lawful-intercept ssdf

Refer to the *Lawful Intercept Guide* for a description of this command.

link-aggregation port switch to

When a link aggregation group (LAG) contains two sets of ports with each connecting to a different Ethernet switch, this command allows you to change the status of the active distributing ports.

Default: none.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

link-aggregation port switch to *slot#* **/** *port#*

slot#

Identifies the physical chassis slot where the line card is installed.

port#

Identifies the physical port on the line card to automatically switch to.

Usage

This command is subject to the following restrictions:

- *slot#/port#* must support LAG.
- *slot#/port#* must be configured with LAG.
- *slot#/port#* must not be actively distributing.
- *slot#/port#* must have negotiated a partner while in standard mode.
- *slot#/port#*'s partner must have a priority equal to or greater than itself.
- *slot#/port#*'s partner bundle must have bandwidth in standard mode equal to or greater than itself.
- Switching to *slot#/port#* must not violate preference within hold-time in standard mode.

Example

```
link-aggregation port switch to 17/2
```

logging active

Enables or disables logging for active internal log files.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
logging active [ copy runtime filters ] [ event-verbosity event_level ] [ pdu-data format
] [ pdu-verbosity pdu_level ]

no logging active
```

no

Indicates the internal logging is to be disabled.

copy runtime filters

Copies the runtime filters and uses that copy to filter the current logging session.

event-verbosity *event_level*

Specifies the level of verboseness to use in logging of events as one of:

- *min*: Displays minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.
- *concise*: Displays detailed information about the event, but does not provide the event source within the system.
- *full*: Displays detailed information about event, including source information, identifying where within the system the event was generated.

pdu-data *format*

Specifies output format for packet data units when logged as one of:

- *none*: raw format (unformatted).
- *hex*: hexadecimal format.
- *hex-ascii*: hexadecimal and ASCII similar to a main-frame dump.

pdu-verbosity *pdu_level*

Specifies the level of verboseness to use in logging of packet data units as an integer from 1 through 5, where 5 is the most detailed.

Usage

Adjust the active logging levels when excessive log file sizes are being generated or, conversely, not enough information is being sent to the active log files for adequate troubleshooting support. The **no** keyword is used to disable internal logging.

Important: A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.

Important: Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.

Example

The following sets the active logging for events to the maximum.

```
logging active event-verbosity full
```

The following command sets the active logging for packet data units to level *3* and sets the output format to the main-frame style *hex-ascii*.

```
logging active pdu-data hex-ascii pdu-verbosity 3
```

The following disables internal logging.

```
no logging active
```

logging filter

Sets the logging filtering options for all or individual facilities.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
logging filter active facility facility level severity_level [ critical-info | no-
critical-info ]
```

active

Indicates only active processes are to have logging options set.

facility *facility*

Specifies the facility to modify the filtering of logged information. Valid facilities for this command are:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: AAA client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **aal2**: AAL2 protocol logging facility
- **acl-log**: Access Control List logging facility
- **acsctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: Active Charging Service (ACS) Manager facility
- **alarmctrl**: Alarm Controller facility
- **alcap**: ALCAP protocol logging facility
- **alcapmgr**: ALCAPMgr logging facility
- **all**: All facilities
- **asngwmgr**: ASN Gateway Manager facility
- **asnpcmgr**: ASN Paging Controller Manager facility
- **bfd**: BFD protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux-De-mux Manager logging facility
- **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)

- **callhome**: Call home application logging facility
- **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
- **cli**: CLI logging facility
- **credit-control**: Credit Control facility
- **cscf**: IMS/MMD CSCF
- **cscfmgr**: SIP CSCF Manager facility
- **cscfttmgr**: SIP CSCFTT Manager facility
- **csp**: Card Slot Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: Content Service Selection (CSS) RADIUS Signaling facility
- **cx-diameter**: Cx Diameter Messages facility
- **dcardctrl**: IPSEC Daughter Card Controller logging facility
- **dcardmgr**: IPSEC Daughter Card Manager logging facility
- **demuxmgr**: Demux Manager API facility
- **dgmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol logging facility
- **dhcpv6**: DHCPv6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages facility
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting
- **diameter-auth**: Diameter Authentication
- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ACS Diameter signaling facility
- **diameter-hdd**: Diameter HDD Interface facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSEC Data Path facility
- **drvctrl**: Driver Controller facility
- **eap-ipsec**: EAP
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface facility
- **egtpc**: eGTP-C logging facility
- **egtpmgr**: eGTP manager logging facility
- **egtpu**: eGTP-U logging facility
- **epdg**: ePDG logging facility

- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
- **fng**: FNG logging facility
- **gmm**:
  - For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
  - For 3G: Logs the access application layer (above the RANAP layer)
- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
- **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
- **gss-gcdr**: GTPP Storage Server GCDR facility
- **gtpc**: GTP-C protocol logging facility
- **gtpcmgr**: GTP-C protocol Manager logging facility
- **gtpp**: GTP-PRIME protocol logging facility
- **gtpu**: GTP-U protocol logging facility
- **gtpumgr**: GTPU Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages facility
- **gy-diameter**: Gy Diameter messages facility
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **hdctrl**: HD Controller logging facility
- **hnb-gw**: HNB-GW (3G Femto GW) logging facility
- **hnbmgr**: HNBMGR (3G Femto GW DemuxMgr) logging facility
- **hss-peer-service**: HSS Peer Service facility
- **igmp**: IGMP
- **ikev2**: IKEv2
- **ims-authorizatn**: IMS Authorization Service facility
- **ims-sh**: HSS SH Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **imsue**: IMSUE
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipms**: IPMS logging facility
- **ipsec**: IP Security logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility

- **ipsp**: IP Pool Sharing Protocol logging facility
- **kvstore**: KV Store facility
- **l2tp-control**: L2TP control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: LAGMGR logging facility
- **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
- **li**: Refer to the *Lawful Intercept Interface Reference* for a description of this command.
- **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
- **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
- **local-policy**: Local Policy Service facility
- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway manager logging facility
- **map**: MAP Protocol logging facility
- **megadiammgr**: Megadiameter Manager (SLF Service) logging facility
- **mme-app**: Mobility Management Entity Application logging facility
- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: Mobility Management Entity Demux Manager logging facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 logging facility
- **mpls**: MPLS protocol logging facility
- **mseg-app**: MSEG application logging facility
- **mseg-gtpc**: MSEG GTPC application logging facility
- **mseg-gtpu**: MSEG GTPU application logging facility
- **msegmgr**: MSEGMgr (MSEG DemuxMgr) logging facility
- **mtp2**: MTP2 Service logging facility
- **mtp3**: MTP3 Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **npuctrl**: Network Processor Unit Control facility
- **npumgr**: Network Processor Unit Manager facility
- **npumgr-acl**: NPUMGR ACL logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility

- **npumgr-fwd**: NPUMGR FWD logging facility
- **npumgr-init**: NPUMGR INIT logging facility
- **npumgr-port**: NPUMGR PORT logging facility
- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **ntfy-intf**: Notification Interface logging facility
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF protocol logging facility
- **ospfv3**: OSPFv3 protocol logging facility
- **p2p**: Peer-to-Peer Detection logging facility
- **pccmgr**: IPCF PCC Manager library
- **pdg**: PDG logging facility
- **pdgdmgr**: PDG Demux Manager logging facility
- **pdif**: PDIF logging facility
- **pgw**: PDN Gateway logging facility
- **phs**: Payload Header Suppression
- **phs-control**: PHS X1/X5 and X2/X6 Interface logging facility
- **phs-data**: PHS Data logging facility
- **phs-eapol**: PHS EAPOL logging facility
- **phsgwmgr**: PHS Gateway Manager facility
- **phspcmgr**: PHS Paging Controller Manager facility
- **pmm-app**: PMM application logging facility
- **ppp**: PPP link and packet facilities
- **pppoe**: PPPOE logging facility
- **push**: VPNMGR CDR push logging facility
- **radius-acct**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Rf Diameter messages facility
- **rip**: RIP logging facility (RIP is not supported at this time.)
- **rohc**: RObust Header Compression facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RUA (3G Femto GW - RUA messages) logging facility

- **s1ap**: S1AP Protocol logging facility
- **sccp:** SCCP Protocol logging connection-oriented messages between RANAP and TCAP layers.
- **sct**: Shared Configuration Task logging facility
- **sctp**: SCTP Protocol logging facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN 'glue' interfaces, e.g., between PMM, MAP,. GPRS-FSM, SMS.
- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN MBMS Bearer app (SMGR) logging facility
- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSNs System Components logging facility; used infrequently
- **sgsn-test**: SGSN Tests logging facility; used infrequently
- **sgtpcmgr**: SGSN GTPC Manager logging information exchange through SGTPC and the GGSN
- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages facility
- **sitmain**: System Initialization Task main logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
- **sndcp**: SNDCP Protocol logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF SPR Manager logging facility
- **srdb**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **sscfnni**: SSCFNNI Protocol logging facility
- **sscop**: SSCOP Protocol logging facility
- **ssh-ipsec**: SSH IP Security logging facility
- **ssl**: SSL (Secure socket layer messages) logging facility
- **stat**: Statistics logging facility
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **tcap**: TCAP Protocol logging facility

- **testctrl**: Test Controller logging facility
- **testmgr**: Test Manager logging facility
- **threshold**: threshold logging facility
- **ttg**: TTG logging facility
- **tucl**: TUCL logging facility
- **udr**: User detail record facility (used with the Charging Service)
- **user-data**: User data logging facility
- **user-l3tunnel**: User layer-3 tunnel logging facility
- **usertcp-stack**: User TCP Stack
- **vpn**: Virtual Private Network logging facility
- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6

---

level *severity_level*

Specifies the level of information to be logged from the following list which is ordered from highest to lowest:

- critical - display critical events
- error - display error events and all events with a higher severity level
- warning - display warning events and all events with a higher severity level
- unusual - display unusual events and all events with a higher severity level
- info - display info events and all events with a higher severity level
- trace - display trace events and all events with a higher severity level
- debug - display all events

---

critical-info | no-critical-info

critical-info: Specifies that events with a category attribute of critical information are to be displayed. Examples of these types of events can be seen at bootup when system processes and tasks are being initiated. This is the default setting.
no-critical-info: Specifies that events with a category attribute of critical information are not to be displayed.

Usage

Apply filters for logged data to collect only that data which is of interest.

Important: A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.

Important: Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.

Caution: Issuing this command could negatively impact system performance depending on the amount of system activity at the time of execution and/or the type of facility(ies) being logged.

Example

The following are selected examples used to illustrate the various options. Not all facilities will be explicitly shown as each follows the same syntax for options.
The following sets the level to log only *warning* information for *all* facilities.

```
logging filter active facility all level warning
```

The following enables the logging of critical information for the SNMP facility while setting the level to *error*.

```
logging filter active facility snmp level error critical-info
```

logging trace

Enables or disables the logging of trace information for specific calls, mobiles, or network addresses.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

logging trace { **callid** *call_id* | **ipaddr** *ip_address* | **msid** *ms_id* | **username** *user_name* }

no logging trace { **callid** *call_id* | **ipaddr** *ip_address* | **msid** *ms_id* | **username** *user_name* }

no

Indicates the logging of trace information is to be disabled.

callid *call_id* **| ipaddr** *ip_address* **| msid** *ms_id* **| username** *user_name*

callid *call_id*: Specifies the exact call instance ID which is to have trace data logged.as a 4-byte hexadecimal number.
ipaddr *ip_address*: Specifies the IP address in IPv4 dotted-decimal notation for which trace information is to be logged.
msid *ms_id*: Specifies the mobile subscriber ID for which trace information is to be logged as 7 to 16 digits of an IMSI, MIN, or RMI.
username *user_name*: Specifies a previously configured user who is to have trace information logged.

Usage

A trace log is useful in troubleshooting subscriber problems as well as for system verification by using a test subscriber. The **no** keyword is used to stop the logging of trace information.

Important: A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.

Important: Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.

Caution: Issuing this command could negatively impact system performance depending on the number of subscribers connected and the amount of data being passed.

Example

The following commands enables/disables trace information for user *user1*.

```
logging trace username user1no logging trace username user1
```

The following commands will enable/disable trace information logging for the user assigned IP address *10.2.3.4*.

```
logging trace ipaddr 10.2.3.4no logging trace ipaddr 10.2.3.4
```

The following enables/disables logging of trace information for call ID *fe80AA12*.

```
logging trace callid fe80AA12no logging trace callid fe80AA12
```

logs checkpoint

Performs check pointing operations on log data. Check pointing identifies logged data as previously viewed or marked. Check pointing results in only the log information since the last check point being displayed; check pointed log data is not available for viewing.

Individual logs may have up to 50,000 events in the active log. Check pointing the logs will then result in at most 50,000 events being in the inactive log files. This gives a maximum of 100,000 events in total which are available for each facility logged.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
logs checkpoint
```

Usage

Check point log data to a set the log contents to a well know point prior to special activities taking place. This command may also be a part of periodic regular maintenance to manage log data.
The check pointing of logs moves the current log data to the inactive logs. Only the most recently check pointed data is retained in the inactive logs. A subsequent check pointing of the logs will result in the prior check pointed inactive log data being cleared and replaced with the newly check pointed data.
The check pointing of log data moves the active log data to be retained as the inactive log data. This results in the active log data, if displayed, having no data earlier than the point in time when the check pointing occurred.

Important: Check pointing of logs should be done periodically to avoid the logs becoming full. Logs which have 50,000 events logged will discard the oldest events first when new events are to be logged.

Example

```
logs checkpoint
```

lsp-ping

Checks Multi Protocol Label Switching (MPLS) label switch path (LSP) connectivity for the specified forwarding equivalence class (FEC). It must be followed by an IPv4 FEC prefix.

Product

All

Privilege

Security Administrator, Administrator

Syntax

lsp-ping *ip_prefix_FEC* [**count** *ping_packets*] [| **verbose**] [| **grep** *grep_options*]

ip_prefix_FEC

is an IPv4 prefix FEC with or without subnet mask entered using IPv4 dotted-decimal or CIDR notation.

count *ping_packets*

Sets the number of ping packets to be sent as an integer from 1 through 16. Default: 4.

Important: The timeout interval for the packets is 5 seconds by default.

verbose

Sets the verbose (detailed) output mode.

grep*grep_options*

Pipes (sends) the output of this command to the **grep** command.

Usage

This command is used to verify the MPLS LSP connectivity for the specified FEC.

Example

Following are the examples for using this command with all possible options for IPv4 address *13.13.13.1* and mask *32* (CIDR notation):

```
lsp-ping 13.13.13.1/32

lsp-ping 13.13.13.1/32 count 15

lsp-ping 13.13.13.1/32 verbose
```

lsp-traceroute

Discovers MPLS LSP routes that packets actually take when traveling to their destinations. It must be followed by an IPv4 or IPv6 FEC prefix.

Product

All

Privilege

Security Administrator, Administrator

Syntax

lsp-traceroute *ip_prefix_FEC* [**maxttl** *time_to_live*] [| **verbose**] [| **grep** *grep_options*]

ip_prefix_FEC

Specifies the destination IP address in IPv4 dotted-decimal or IPv6 colon-separated with or without mask (CIDR notation).

maxttl *time_to_live*

Sets the maximum time to live in hops. TTL is an integer from 1 through 255. Default: 30.

verbose

Sets the verbose (detailed) output mode.

grep*grep_options*

Pipes (sends) the output of this command to the **grep** command.

Usage

This command is used or the router to discover the MPLS LSP routes through which the packets will travel to their IPv4 destinations.

Example

The following command specifies the destination IP address *13.13.13.13* for which the MPLS routes will be discovered for packets to traverse:

```
lsp-traceroute 13.13.13.13/32
```

mkdir

Creates a new directory in the local file system or in remote locations as specified.

Product

All

Privilege

Security Administrator, Administrator

Syntax

mkdir *filepath*

filepath

Specifies the directory path to create. The path must be formatted as follows:
`[file: ]{ /flash | /pcmcia1 | /hd }[ /directory ]/file_name`

Important: Use of the SMC hard drive is not supported in this release.

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name
filename is the actual file of interest

Usage

Create new directories as part of periodic maintenance activities to better organize stored files.

Example

The following creates the directory */flash/pub* in the local flash storage.

```
mkdir /flash/pub
```

mme offload

Initiates or stops the offload of UEs associated with a specified MME service.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

mme offload mme-service *name* **{ start mme-init-release-timeout** *seconds* **paging-init-timeout** *seconds* **| stop }**

mme-service *name*

Specifies the name of an existing MME service from which UEs will be offloaded as an alphanumeric string of 1 trough 63 characters.

start mme-init-release-timeout *seconds* **paging-init-timeout** *seconds* **| stop } [-noconfirm]**

Sets the timeout for the initial release procedure and the paging procedure.
start mme-init-release-timeout *seconds*: Configures the timeout (in seconds) for triggering the IDLE MODE ENTRY procedure for UEs that are in the ECM_CONNECTED state as an integer from 1 to 120. The cause of the IDLE MODE ENTRY will be "Load balancing TAU required".
paging-init-timeout *seconds*: Configures the timeout (in seconds) for triggering the PAGING procedure for UEs in the ECM_IDLE state as an integer from 1 to 120. After returning the UEs to the ECM_CONNECTED state, the IDLE MODE ENTRY procedure is triggered with the "Load balancing TAU required" cause.
stop: Ends the off-load process.

-noconfirm

Executes the command without any additional prompts or confirmation from the user.

Usage

Use this command to initiate or stop the off-loading of UEs associated with a specified MME service.

Important: If all subscribers are to be off-loaded, and prior to initiating this command, you must set the **relative-capacity** command in the MME Service Configuration Mode to zero (0). This allows all new calls to be re-directed to other MMEs in the pool while existing calls on the off-loading MME are removed.

Example

The following command sets the trigger to start off-loading UEs from a service named *mme3* at *60* seconds and the paging trigger at *90* seconds:

```
mme offload mme-service mme3 start mme-init-release-timeout 60 paging-
init-timeout 90
```

mme reset

Sends an S1 RESET message to a designated EnodeB to reset all UE-associated S1 connections.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

mme reset s1-peer *peer_ID*

s1-peer *peer-ID*

Specifies an existing EnodeB peer ID to which the REST message is to be sent as an integer from 1 through 4294967295.

Usage

Use this command to send an S1 RESET message to a designated EnodeB to reset all UE-associated S1 connections.
The S1 peer ID for an EnodeB can be identified by executing the **show mme-service enodeb-association** command available in this mode. The peer ID is presented in the "Peerid" field.

Example

The following command initiates the sending of an S1-peer reset message to an EnodeB with a peer ID of *22315734*:

```
mme rest s1-peer 22315734
```

monitor protocol

Enters the system's protocol monitoring utility.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
monitor protocol
```

Usage

Useful for troubleshooting, this command provides a tool for monitoring protocol transactions between the system and other network nodes including the mobile station(s).
The following protocols can be monitored:

- SNMP
- RADIUS Authentication
- RADIUS Accounting
- A11 (R-P Interface) (PDSN only)
- Mobile IPv4
- A11MGR
- PPP
- A10
- User L3 (User Layer 3 protocols)
- USERTCP STACK
- L2TP
- L2TPMGR
- L2TP Data
- GTPC
- GTPCMGR
- GTPU
- GTPP

Important: If the hard disk drive (HDD) is used for CDR storage, the CDR option must be used and not GTPP option (27).

- DHCP (GGSN only)
- CDR
- DHCPV6

- MIP Tunnel
- L3 Tunnel (Layer 3 Tunnel Protocols)
- CSS Data
- CSS Signaling

> ***Important:*** In StarOS 9.0 and later releases the CSS Data Signaling option is not supported.

- EC Diameter (Diameter Enhanced Charging)
- SIP (IMS)
- IPSec IKE Inter-Node
- IPSec IKE Subscriber
- IPSG RADIUS Signal
- ROHC (Robust Header Compression)
- WiMAX R6
- WiMAX Data
- SRP
- BCMCS SERV AUTH
- RSVP
- Mobile IPv6
- ASNGWMGR
- STUN
- SCTP: Enabling this option will display the SCTP protocol message packets on HNB-GW node.
- M3UA
- SCCP
- TCAP
- MAP
- RANAP
- GMM
- GPRS-NS
- BSSGP
- CAP
- SSCOP
- SSCFNNI
- MTP3
- LLC
- SNDCP
- BSSAP+

- SMS
- PHS-Control (Payload Header Compression)
- PHS-Data
- DNS Client
- MTP2
- HNBAP: Enabling this option will display the HNB Application Part (HNBAP) protocol packets.
- RUA: Enabling this option will display the RANAP User Adaptation (RUA) protocol packets.
- EGTPC
- App Specific Diameter
- PHS-EAPOL
- ICAP
- Micro-Tunnel
- ALCAP: Enabling this option will display the Access Link Control Application Part (ALCAP) protocol message packets on HNB-GW node.
- SSL
- S1-AP
- NAS
- LDAP
- SGS
- AAL2: Enabling this option will display the ATM Adaptation Layer 2 (AAL2) protocol message packets on HNB-GW node.
- PHS (Payload Header Suppression)
- PPPOE
- RTP (IMS)
- RTCP (IMS)

Once the protocol has been selected, the utility monitors and displays every relative protocol message transaction.
Protocol monitoring is performed on a context-by-context-basis. Therefore, the messages displayed are only those that are transmitted/received within the system context from which the utility was executed.
For additional information on using the monitor utility, refer to the *System Amdinistration Guide*.

Caution: Protocol monitoring can be intrusive to subscriber sessions and could impact system performance. Therefore, it should only be used as a troubleshooting tool.

Example

The following command opens the *protocol* monitoring utility:

```
monitor protocol
```

monitor subscriber

Enables the system's subscriber monitoring utility. Available keywords vary based on the licenses installed on the system.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

monitor subscriber [asn-peer-address *bs_peer_address* **| callid** *call_id* **fng-peer-address** *ipv4_address* **| imei** *imei_value* **| imsi** *imsi_value* **| ipaddr** *ip_address* **| ipv6addr** *ipv6_address* **| ipsg-peer-address** *ipsg_peer_address*| **msid** *ms_id* **| msisdn** *msisdn* **| next-call | pcf** *pcf_address* **| pdif-peer-address** *pdif_peer_address* **| peer-fa** *peer_fa_address* **| peer-lac** *lac_peer_address* **| sgsn-address** *sgsn_address* **| type { 1xrtt | asngw | asnpc | closedrp | evdorev0 | evdoreva | interrogating-cscf | ggsn [Next-Call By APN] | ha | ipsg | lns | mme | pdif | proxy-cscf | rfc3261-proxy | serving-cscf } next-call | type bcmcs { next-call | next-service-request } | username** *user_name*| **Next-Call By APN]**

asn-peer-address *bs_peer_address*

Specifies the peer ASN Base Station IP address in IPv4 address in dotted-decimal notation.

callid *call_id*

Specifies the call identification number assigned to the subscriber session by the system to be monitored as a 4-byte hexadecimal number.

fng-peer-address *ipv4_address*

Specifies the specific FNG WLAN IP address in IPv4 dotted-decimal notation.

imei *imei_value*

International Mobile Equipment Identification (IMEI). Must be followed by 8 digits of TAC (Type Allocation Code) and 6 digits of SNR (Serial Number). Only the first 14 digit of IMEI/IMEISV is used to find the equipment ID.

imsi *imsi_value*

Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session to be monitored an integer from 1 though 15 characters.

ipaddr *ip_address*

Specifies the IP address of the subscriber session to be monitored in IPv4 dotted-decimal notation.

ipv6addr *ipv6_address*

Specifies the IPv6 address of the subscriber session to be monitored in IPv6 colon-separated notation.

ipsg-peer-address *ipsg_peer_address*

Specifies the peer IPSG IP address. Must be followed by an IPv4 address in dotted -decimal notation.

msid *ms_id*

Specifies the mobile subscriber identification number to be monitored as 7 to 16 digits of an IMSI, MIN, or RMI.

msisdn *msisdn*

Specifies the Mobile Subscriber ISDN number to be monitored as 7 to 16 digits of an IMSI, MIN, or RMI.

next-call

Specifies that the system will monitor the next incoming subscriber session.
Entering this keyword will display the available options of protocols to select. For a list of supported protocols with this keyword, refer to the **monitor protocol** command.

pcf *pcf_address*

Specifies the PCF IP address in IPv4 dotted-decimal notation.

pdif-peer-address *pdif_peer_address*

Specifies the peer PDIF IP address in IPV4 dotted-decimal notation.

peer-fa *peer_fa_address*

Specifies the peer FA IP address in IPv4 dotted-decimal notation.

peer-lac *lac_peer_address*

Specifies the peer LAC IP address in IPv4 dotted-decimal notation.

sgsn-address *sgsn_address*

Specifies the SGSN IP address in IPv4 dotted-decimal notation.

type { 1xrtt | asngw | asnpc | evdorev0 | evdoreva | | fng | interrogating-cscf | ggsn [Next-Call By APN] | ha | ipsg | lns | mme | openrp | | pdif | proxy-cscf | rfc3261-proxy | serving-cscf } next-call

Allows monitoring for specific subscriber types established in the system when next call occurs.

- **1xrtt**: Displays logs for cdma2000 1xRTT call session subscriber
- **asngw**: Displays logs for ASN-GW call session subscriber
- **asnpc**: Displays logs for ASN PC/LR call session subscriber
- **evdorev0**: Displays logs for cdma2000 EVDO Rev0 call session subscriber
- **evdoreva**: Displays logs for cdma2000 EVDO RevA call session subscriber
- **fng**: Displays logs for the FNG session subscriber
- **interrogating-cscf**: Displays logs for Interrogating CSCF subscriber
- **ggsn**: Displays logs for UMTS GGSN call session subscriber

- **Next-Call By APN**: Display logs for next call on APN basis, where APN name can be any Gi or Gn APN.
- **ha**: Displays logs for Home Agent call session subscriber
- **ipsg**: Displays logs for IPSG call session subscriber
- **lns**: Displays logs for LNS call session subscriber
- **mme**: Displays logs for MME session subscribers.
- **pdif**: Displays logs for PDIF call session subscriber
- **proxy-cscf**: Displays logs for Proxy CSCF subscriber
- **rfc3261-proxy-cscf**: Displays logs for non-ims-proxy (RFC-3261 proxy) subscriber
- **serving-cscf**: Displays logs for Serving CSCF subscriber

type bcmcs {*next-call* | *next-service-request***}**

Specifies the type of BCMCS call for the subscriber.

username *user_name*

Specifies the username of an existing subscriber to be monitored.

Usage

The monitor subscriber utility provides a useful tool for monitoring information about and the activity of either a single subscriber or all subscribers with active sessions within a given context.
The following items can be monitored:

- Control events
- Data events
- Event ID information
- Inbound events
- Outbound events
- Protocols (identical to those monitored by command)

Once the criteria has been selected, the utility will monitor and display every relative piece of information on the subscriber(s).
For additional information on using the monitor utility, refer to the *System Amdinistration Guide*.

Important: Option Y for performing multi-call traces is only supported for use with the GGSN. This option is available when monitoring is performed using the “Next-Call” option. It allows you monitor up to 11 primary PDP contexts for a single subscriber.

Subscriber monitoring is performed on a context-by-context-basis. Therefore, the information displayed will be only that which is collected within the system context from which the utility was executed.

Caution: Subscriber monitoring can be intrusive to subscriber sessions and could impact system performance. Therefore, it should only be used as a troubleshooting tool.

Example

The following command enables monitoring for user *user1*.

```
monitor subscriber username user1
```

The following command will enable monitoring for the user assigned IP address *10.2.3.4*.

```
monitor subscriber ip-address 10.2.3.4
```

The following enables monitoring for call ID *FE80AA12*.

```
monitor subscriber callid fe80aa12
```

newcall policy

Configures new call policies for busy-out conditions.

Product

PDSN, GGSN,, HNB-GW, IPCF, MME, HA, LNS, P-CSCF, ASN-GW, ASN PC/LR, SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

newcall policy { asngw-service | asnpc-service | sgsn-service } { all | name *service_name* **} reject**

newcall policy cscf-service { all | name *service_name* **} { redirect** *target_ip_address* **[weight** *weight_num* **] [** *target_ipaddress2* **[weight** *weight_num* **] ...** *target_ip_address16* **[weight** *weight_num* **] | reject }**

newcall policy { fa-service | lns-service | mipv6ha-service } { all | name *service_name* **} reject**

newcall policy { ha-service | pdsn-service} { all | name *service_name* **} { redirect** *target_ip_address* **[weight** *weight_num* **] [** *target_ipaddress2* **[weight** *weight_num* **] ...** *target_ip_address16* **[weight** *weight_num* **] | reject }**

newcall policy ggsn-service {**apn name** *apn_name* | **all** | **name** *service_name*}**reject**

newcall policy hnbgw-service {**all** | **name** *service_name*}**reject**

newcall policy {**pcc-af-service** | **pcc-policy-service**} {**all** | **name** *service_name*}**reject**

newcall policy mme-service {all | name *service_name* **} reject**

no newcall policy { fa-service | ggsn-service | ha-service | mipv6ha-service | pdsn-service| pdsnclosedrp-service| lns-service } { all | name *service_name* **}**

no newcall policy { ha-service | pdsn-service } { all | name *service_name* **} redirect** *target_ip_address* **[weight***weight_num* **] [** *target_ip_address2* **[weight** *weight_num* **] ...** *target_ip_address16* **[weight***weight_num* **]**

no newcall policy ggsn-service { **apn***apn_name* | **all** | **name** *service_name*} **reject**

no newcall policy { asngw-service | asnpc-service } { all | name *service_name* **}**

no newcall policy hnbgw-service {**all** | **name** *service_name*}

no newcall policy mme-service { all | name *service_name* **}**

no newcall policy {**pcc-af-service** | **pcc-policy-service**} {**all** | **name** *service_name*}

no

Disables the new call policy for all or specified service of a service type.

newcall policy { asngw-service | asnpc-service } { all | name *service_name* **} reject**

Creates a new call policy to reject the calls based on the specified ASN-GW or ASN PC/LR service name or all services of this type.
asngw-service: Specifies the type of service as ASN GW for which new call policy is configured.
asnpc-service: Specifies the type of service as ASN PC/LR for which new call policy is configured.
name *service_name*: Specifies the name of the service for which new call policy is configured. service_name is name of a configured ASN GW or ASN PC/LR service.
reject: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For ASN-GW and ASN PC/LR service rejection code is 81H (Registration Denied - administratively prohibited).

newcall policy { cscf-service | fa-service | lns-service | mipv6ha-service } { all | name *service_name* **} reject**

Creates a new call policy that rejects calls based on the specified access point name.

no newcall policy { cscf-service | fa-service | ggsn-service| ha-service | mipv6ha-service | pdsn-service | } { all | name *service_name* **}**

Removes a previously configured new call policy for the specified service

no newcall policy { ha-service | pdsn-service } { all | name *service_name* **} redirect** *target_ip_address* **[weight** *weight_num* **] [** *target_ip_address2* **[weight** *weight_num* **] ...** *target_ip_address16* **[weight** *weight_num* **]**

Deletes up to 16 IP addresses from the redirect policy. The IP addresses must be expressed in IPv4 dotted-decimal notation

cscf-service | fa-service | ha-service | lns-service | mipv6ha-service | mme-service | pdsn-service | pdsnclosedrp-service

Specifies the type of service for which to configure a new call policy. The following services are supported:

- **cscf-service**: A Call/Session Control Function service
- **fa-service**: A Foreign Agent service
- **ha-service**: A Home Agent service
- **lns-service**: An L2TP Network Server service
- **mipv6ha-service**: A Mobile IPv6 Home Agent service
- **pdsn-service**: A Packet Data Serving Node service

{ all | name *service_name* **}**

Specifies a filter for the new call policy. Whether the new call policy will be applied to all configured services or a specific one.

- **all**: Specifies that the new call policy will be applied to all instances of the selected service type.
- **name**: *service_name*: Specifies the name of a specific instance of the selected service type as an alphanumeric string of 1 through 63 characters that is case sensitive.

redirect *target_ip_address* **[weight** *weight_num* **]** **[** *target_ip_address2* **[weight** *weight_num* **]** ... *target_ip_address16* **[weight** *weight_num* **]**

Configures the busy-out action. When a redirect policy is invoked, the service rejects new sessions and provides the IP address of an alternate destination. This command can be issued multiple times.
target_ip_address# is the IP address of an alternate destination expressed in IPv4 dotted-decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.
weight *weight_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. *weight_num* must be an integer from 1 through 10.
Depending on the type of service that the policy is applied to, the following reason codes are reported as part of the reply:

- **ha service:** 88H (Registration Denied - unknown home agent address)
- **pdsn service:** 88H (Registration Denied - unknown PDSN address)

Important: The redirect option is not supported for use with FA and GGSN services.

newcall policy hnbgw-service { all | name *service_name***} reject**

Creates a new call policy to reject the calls in a specified HNB-GW service name instance or all HNB-GW services on the system.
name *service_name*: Specifies the name of the HNB-GW service for which new call policy is configured.
reject: Specifies that the policy rejects all new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For HNB-GW service rejection code is 81H (Registration Denied - administratively prohibited).

newcall policy mme-service { all | name *service_name* **} reject**

Creates a new call policy to reject the calls based on the specified MME service name or all MME services on the system.
name *service_name*: Specifies the name of the MME service for which new call policy is configured.
reject: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For MME service rejection code is 81H (Registration Denied - administratively prohibited).

newcall policy {pcc-af-service | pcc-policy-service} {all | name *service_name***}reject**

Creates a new call policy to reject the calls for PCC services on the system for any of the following PCC services:

- **pcc-af-service name** *service_name*: Specifies the Policy and Charging Control-Application Function (PCC-AF) service for which new call policy is to be configured on the system.

  name *service_name*: Specifies the name of an existing PCC-AF service for which new call policy is configured.

- **pcc-policy-service name** *service_name*: Specifies the Policy and Charging Control-Policy (PCC-Policy) service for which new call policy is to be configure on the system.

name *service_name*: Specifies the name of an existing PCC-Policy service for which new call policy is configured.

reject: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For PCC services rejection code is 81H (Registration Denied - administratively prohibited).

reject

Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the following reason codes are reported as part of the reply to indicate the rejection:

- **asngw service**: 81H (Registration Denied - administratively prohibited)
- **fa service:** 41H (administratively prohibited)

Important: When **newcall policy** is set to reject for the FA service, the Busy Bit is set in the Agent Advertisement. Any further RRQs will be rejected with this code value.

- **ggsn service:** C7H (Rejected - no resources available)
- **ha service:** 81H (Registration Denied - administratively prohibited)
- **mipv6ha-service**: 81H (Registration Denied - administratively prohibited)
- **mme service:** 81H (Registration Denied - administratively prohibited)
- **pdsn service:** 81H (Registration Denied - administratively prohibited)

Usage

This command is used to busy-out specific system services prior to planned maintenance or for troubleshooting. This is required when operator find out that the system is somehow overloaded, or needs some kind of maintenances or so.

Example

The following command creates a new call policy to re-direct all new calls for all PDSN services to a device having an IP address of *192.168.1.23*:

```
newcall policy pdsn-service all redirect 192.168.1.23
```

The following command creates a new call policy to reject all new calls for a GGSN service called *ggsn1*:

```
newcall policy ggsn-service name ggsn1 reject
```

The following command creates a new call policy to reject all new calls for an MME service called *MME1*:

```
newcall policy mme-service name MME1 reject
```

The following command creates a new call policy to reject all new calls for an HNB-GW service called *hnbgw1*:

```
newcall policy hnbgw-service name hnbgw1 reject
```

The following command creates a new call policy to reject all new calls for a PCC Policy service called *pcrf1*:

```
newcall policy pcc-policy-service name pcrf1 reject
```

password change

Provides a mechanism for local-user administrative users to change their passwords.

Product

All

Privilege

All local-user administrative levels except as noted below

Syntax

password change [local-user *name* **]**

local-user *name*

Specifies the name of an existing local-user administrative user for which to change the password as an alphanumeric string of 3 through 144 characters that is case sensitive.

Important: This keyword is only available to local-users with an authorization level of security-administrator.

Usage

This command provides a mechanism for local-user administrative users to change their passwords. In addition, it also provides a mechanism for security-administrator local-users to change the password for other local-user accounts.

If the **local-user** keyword is not entered, the system prompts the user for their current password and for the new password. New passwords take effect at the next login. Users that have had their password changed by a security-administrator are prompted to change their passwords at their next login.

New passwords must meet the criteria dictated by the **local-user password** command options in the Global Configuration Mode.

Important: The system does not allow the changing of passwords unless the time limit specified by the **local-user password min-change-interval** has been reached.

Example

The following command, executed by a security-administrator, resets the password for a local-user name *operator12*:

```
password change local-user operator12
```

ping

Verifies ability to communicate with a remote node in the network by passing data packets between and measuring the response. This is accomplished by sending Internet Control Message Protocol (ICMP) echo request packets to the target node (pinging) and waiting for an ICMP response.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Important: Inspector privileges are granted for all variables except **count**. To initiate a ping count, you must have a minimum privilege level of Operator.

Syntax

ping *host* **[broadcast] [count** *num_packets* **] [pattern** *packet_pattern* **] [size** *octet_count* **] [src {** *src_host_name* **|** *src_host_ip_address* **}] [| { grep** *grep_options* **| more }]**

ping *host*

Sends ICMP echo request packets to the remote node specified the node's name (up to 127 alphanumeric characters) or assigned IPv4 address in dotted-decimal notation.

broadcast

Sends ping packets to broadcast addresses.

count *num_packets*

Specifies the number of packets to send to the remote host for verification as an integer from 1 through 10000. Default: 5

pattern *packet_pattern*

Specifies a pattern to use to fill the internet control message protocol packets in hexadecimal format with a value in the range of 0x0000 through 0xFFFF. By default each octet of the packet is encoded with the octet number of the packet.

size *octet_count*

Specifies the number of bytes in each IP datagram as an integer from 40 through 18432. Default: 56

src { src_*host_name* **| src** *host_ip_address* **}**

Specifies an IP address to use in the packets as the source node. Default: originating system's IP address
src_host_name: Specifies the source node using the node's logical host name which must be resolved via DNS lookup.
src_host_ip_address: Specifies the source node using the node's assigned IPv4 address in dotted-decimal notation.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in *Command Line Interface Reference*.

Usage

This command is useful in verifying network routing and if a remote node is able to respond at the IP layer.

Example

The following command is the most basic and will report the results of trying to communication with remote node *remoteABC*.

```
ping remoteABC
```

The following command verifies communication with the remote node *10.2.3.4* using *1000* packets.

```
ping 10.2.3.4 count 1000
```

The following command verifies communication with remote node *remoteABC* while making it appears as though the source is remote node with IP address *10.2.3.4*.

```
ping remoteABC src 10.2.3.4
```

Important: The responses from the remote host to the ping packets will be rerouted to the host specified as the source.

ping6

Specifies ping options for IPv6 addresses.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

ping6 { *hostname* **|** *ipv6 address* **} [count** *num* **] [flood] [pattern** *val* **] [size** *val* **] [src** *ip_address* **] [interface** *string* **] [vrf** *vrf_name*

hostname

Name of the host to be pinged.

ipv6 address

IPv6 address of host to be pinged in colon-separated notation.

count*num*

Sets the number of ping packets to be sent as an integer from 1 through 10000.

flood

Configures ping6 to send packets as quickly as possible, or 100 per second, whichever is faster.

pattern *val*

Specifies the hexadecimal pattern to fill ICMP packets as a hexadecimal number from 0x0 through 0ffff

size *val*

Specifies the size of ICMP datagram (in bytes) as an integer from 40 through 18432. Default: 56.

src *ip_address*

Specifies the source IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.

interface *string*

Specifies the originating source interface name as an alphanumeric string of 1 through 79 characters.

vrf *name*

Specifies the name of an existing VFR as an alphanumeric string of 1 through 63 characters.

Usage

Ping command for IPv6. Note that the command is just “ping6, and not “pingv6.”

Example

Use this command to ping the IPv6 address *2001:0db8:85a3:0000:0000:8a2e:0370:7334*

```
ping6 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

port switch to

Performs a manual switchover to an available redundant/standby line card or SPIO port.

Default: none.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

port switch to *slot#* **/** *port#*

slot#

Identifies the physical chassis slot where the line card or SPIO card is installed.

port#

Identifies the physical port on the line card or SPIO to automatically switch to.

Usage

This command is used to specify the redundant port on a Line Card (LC). When port redundancy is enabled, if an external network device or cable failure occurs that causes a link down failure on the port, then the redundant port is used.

Important: This command is not supported on all platforms.

Example

```
port switch to 17/1

port switch to 6/11
```

ppp echo-test

Sends link control protocol (LCP) keep-alive echo packet to the peer point-to-point protocol (PPP) connection to verify proper communication between PPP connections, and awaits a response.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

ppp echo-test { callid *call_id* | **imsi** *imsi_id*use | **ipaddr** *ip_address* | **msid** *ms_id* | **username** *user_name* } [*num_packets*] [| { **grep** *grep_options* | **more** }]

callid *call_id*

Specifies the call instance ID for which the PPP link must be verified as a 4-byte hexadecimal number.

imsi *imsi_id*

Specifies the International Mobile Subscriber Identifier (IMSI) for which the PPP link must be verified.

ipaddr *ip_address*

Specifies the IP address for which the PPP link must be verified in IPv4 dotted-decimal notation.

msid *ms_id*

Specifies the mobile subscriber ID for which the PPP link must be verified as 7 to 16 digits of an MIN, or RMI.

username *user_name*

Specifies an existing user for which the PPP link must be verified as an alphanumeric string of 1 through 127 characters.

num_packets

Specifies the number of test packets to generate an integer from 1 through 1000000. Default: 1

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in *Command Line Interface Reference*.

Usage

Use this command to verify the point-to-point protocol communications. This command sends LCP keep-alive echo packet to the peer PPP connection to verify proper communication between PPP connections. **ppp echo-test** command waits for LCP echo response for configured numbers of tries, if response is not

received it will retry configured no of times with an interval of *5* seconds. This command accepts the parameters call ID, IMSI, IP address, MSID, and user name to specify which active PPP session to consider. **ppp echo-test** command makes the dormant session active.

Caution: Issuing this command could negatively impact system performance depending on the number of subscribers using the same name and/or if the number of packets used in the test is large.

LCP includes Echo-Request and Echo-Reply codes in order to provide a Data Link Layer loopback mechanism for use in exercising both directions of the link. This is useful as an aid in debugging, link quality determination, performance testing, and for numerous other functions. Upon reception of an Echo-Request in the LCP Opened state, an Echo-Reply is transmitted.

Example

The following command tests the PPP link to user *user1*.

```
ppp echo-test username user1
```

The following command tests the PPP link to the user assigned IP address *10.2.3.4*.

```
ppp echo-test ipaddr 10.2.3.4
```

The following tests the PPP link associated with call ID *fe80AA12*.

```
ppp echo-test callid fe80aa12
```

radius interim accounting now

Check points current RADIUS accounting messages immediately.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator

Syntax

```
radius interim accounting now
```

Usage

The interim command may be part of a regiment of periodic activities to maintain the chassis.
This command may also be useful in preparation for system monitoring or troubleshooting to set the list of messages to be displayed at a well known time.

radius test

Verifies the RADIUS servers functions for accounting and authentication.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator

Syntax

radius test { accounting | admin authentication | authentication | probe authentication server *ip_addr* **port** *port_no* **[username** *username* **password** *password* **] } { all | [on] | off] | radius group** *group_name user_name* **| server** *server_name* **port** *server_port* **}** *user_name password*

---

accounting

Tests accounting server functionality.

---

admin authentication *name_admin admin_password*

Tests the RADIUS admin authentication.
name_admin: Specifies he name of the administrator as an alphanumeric string of 1 through 127 characters.
admin_password: Specifies the password for the administrator as an alphanumeric string of 1 through 63 characters.

---

authentication

Tests authentication server functionality.

---

all | radius group *group_name user_name* **| server** *server_name* **port** *server_port*

all: Tests all configured servers.
server *server_name* **port** *server_port*: Tests only the server specified by *server_name* and *server_port*. The server must have been previously configured.
radius group *group_name user_name*: Tests all configured authentication servers in a specific RADIUS group for a specific user. Must be followed by the RADIUS group name and user name.
group_name is an alphanumeric string of 1 through 63 characters that specifies the name of server group configured in the specific context for authentication/accounting.

---

on/off

Allows the user to turn RADIUS test accounting on or off.

---

user_name

Specifies the RADIUS user who is to be verified. The user must have been previously configured.

---

password

Specifies the RADIUS user who is to have authentication verified. *password* is only applicable when the **authentication** keyword is specified.

Usage

Test the RADIUS accounting for troubleshooting the system for specific users or to verify all the system RADIUS accounting functions.

Example

The following verifies all RADIUS servers.

```
radius test accounting all

radius test authentication all
```

The following verifies the RADIUS accounting and authentication for user *user1* for the *sampleServer*.

```
radius test accounting server sampleServer port 5000 user1

radius test authentication server sampleServer port 5000 user1 dumyPwd
```

The following commands will verify the RADIUS accounting and authentication for RADIUS server group *star1* for the current context:

```
radius test accounting server sampleServer port 5000 user1

radius test authentication server sampleServer port 5000 user1 dummyPwd

radius test authentication all
```

The following verifies the RADIUS authentication server group *star1* for user *user1*.

```
radius test authentication radius group star1 user1
```

reload

Invokes a full system reboot. All processes are terminated and the system initiates a hardware reset (reboot). This command is identical to the **shutdown** command.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
reload [ -noconfirm ]
```

-noconfirm

Executes the command without any additional prompts or confirmation from the user.

Usage

The system performs a hardware reset and reloads the highest priority boot image and configuration file specified in the boot.sys file. Refer to the **boot system priority** command in the Global Configuration Mode for additional information on configuring boot images, configuration files and priorities.

Important: To avoid the abrupt termination of subscriber sessions, it is recommended that a new call policy be configured and executed prior to invoking the **reload** command. This policy sets busy-out conditions for the system and allows active sessions to terminate gracefully. Refer to the **newcall** command in the Exec Mode for additional information.

Caution: Issuing this command causes the system to become unavailable for session processing until the reboot process is complete.

Example

The following command performs a hardware reset on the system:

```
reload
```

rename

Changes the name of an existing local file.

Product

All

Privilege

Security Administrator, Administrator

Syntax

rename *from_filepath to_filepath* **[-noconfirm]**

from_filepath

Specifies the path to the file/directory to be renamed. The path must be formatted according to the following format:
`[file: ]{ /flash | /pcmcia1 | /hd }[ /directory ]/file_name`

Important: Use of the SMC hard drive is not supported in this release.

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name
filename is the actual file of interest

to_filepath

Specifies the new name of file/directory. The path must be formatted as follows:
`[file: ]{ /flash | /pcmcia1 | /hd }[ /directory ]/file_name`

Important: Use of the SMC hard drive is not supported in this release.

directory is the directory name
filename is the actual file of interest

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Important: Extreme caution should be taken when using the **-noconfirm** option. The paths to the source and the destination should be verified prior to performing the command.

Usage

Rename files as part of regular system maintenance in conjunction with the delete command.

Example

The following renames the directory */pub* in the local PCMCIA1 device.

```
rename /pcmcia1/pub /pcmcia1/pub_old
```

reveal disabled commands

Enables or disables the input of commands for features that do not have license keys installed. The output of the command **show cli** indicates when this feature is enabled. This command effects the current CLI session only and is disabled by default.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

```
[ no ] reveal disabled commands
```

no

Does not show disabled commands.

reveal disabled commands

Shows disabled commands.

Usage

When this command is enabled and a disabled command is entered, a message is displayed that informs you that the required feature is not enabled and also lists the name of the feature that you need to support the command.
When this command is disabled and a disabled command is entered, the CLI does not acknowledge the existence of the command and displays a message that the keyword is unrecognized.

Example

The following command sets the CLI to accept disabled commands and display the required feature for the current CLI session with the following command:

```
reveal disabled commands
```

The following command sets the CLI to reject disabled commands and return an error message for the current CLI session:

```
no reveal disabled commands
```

rlogin

Attempts to connect to a remote host.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

rlogin { *host_name* | *host_ip_address* } [user *user_name*]

host_name* | *host_ip_address

Identifies the remote node with which to attempt connection.
host_name: Specifies the remote node using the node's logical host name which must be resolved via DNS lookup.
host_ip_address: Specifies the remote node using its assigned IP address in IPv4 dotted-decimal notation.

user *user_name*

Specifies a user name attempting connection as an alphanumeric string of 1 through 1023 characters.

Usage

Connect to remote network elements using rlogin.

Important: **rlogin** is not a secure method of connecting to a remote host. **ssh** should be used whenever possible for security reasons.

Example

The following connects to remote host *remoteABC* as user *user1*.

```
rlogin remoteABC user user1
```

The following connects to remote host *10.2.3.4* without any default user.

```
rlogin 10.2.3.4
```

rmdir

Removes (deletes) a local directory.

Product

All

Privilege

Security Administrator, Administrator

Syntax

rmdir *path* **[force]**

path

Specifies the directory path to remove. The must be formatted according as follows:
[**file:**]{ **/flash** | **/pcmcia1** | **/hd** }[**/***directory*]**/***file_name*

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name
filename is the actual file of interest

force

Over-rides any warnings to force deletion of the directory and any files contained therein.

Important: Use of the **force** keyword should be done with care to ensure the directory is specified accurately as there is no method to recover a directory which has been removed.

Usage

Remove old directories as part of regular maintenance.

Example

The following removes the local directory */pcmcia1/pub*.

```
rmdir /pcmcia1/pub
```

rotate-hd-file

Rotates the Diameter files stored on the hard disk drive.

Product

SGW, PGW, HSGW

Privilege

Security Administrator, Administrator

Syntax

rotate-hd-file diameter [name *policy_name* **]**

name *policy_name*

Specifies the hd-storage policy name of an existing HD Storage Policy as an alphanumeric string of 0 through 63 characters.

Usage

Use this command to manually rotate the Diameter HD stored files.

Example

The following command rotates Diameter files that were stored using the HD storage policy named CDR1:

rotate-hd-file diameter name *CDR1*

save configuration

Saves the configuration of current contexts to a local or remote location. The configuration contains the sequence of CLI commands that define system parameters and ends with the **.cfg** extension.

Product

All

Privilege

Security Administrator, Administrator

Syntax

save configuration *url* **[obsolete-encryption |showsecrets | verbose] [-redundant] [-noconfirm]**

url

Default: saves to the location of the active configuration currently loaded.
Specifies the location in which to store the configuration file. *url* may refer to a local or a remote file and must be entered in the following format:
[file:] { /flash | /pcmcia1 | /hd-raid } [/*directory***] /***file_name***
tftp:// {** *host* **[:** *port#* **] } [/***directory***] /***file_name***
[ftp: | sftp:] // [** *username* **[:***password***] @] {** *host* **} [:** *port#* **] [/***directory***] /** *file_name*

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.

Important: *hostname* can **only** be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserver.

port# is the logical port number that the communication protocol is to use.

[obsolete-encryption |showsecrets | verbose]

Specifies options when saving the configuration file.

obsolete-encryption: Saves the configuration with encrypted values generated via an obsolete encryption method. This option may be required to preserve a configuration for a possible downgrade.

showsecrets: Saves the CLI configuration file with all passwords in plain text, rather than their default encrypted format.

verbose: Saves as much information as possible, including default values. If this option is not specified, the configuration will not include default values.

-redundant

Saves the configuration file to the local device on the System Management Card (SMC), defined by the *url* variable, and then automatically copies that same file to the like device on the standby SMC, if available.

Important: This keyword will only work for local devices that are located on both the active and standby SMCs. For example, if you save the file to the **/pcmcia1** device on the active SMC, that same type of device (**pcmcia1**) must be available on the standby SMC. Otherwise, a failure message is displayed. When saving the file to an external network (non-local) device, the system disregards this keyword.

Important: This keyword does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active SMC, then you must synchronize the local file system on both SMCs.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Important: Exercise caution when using the **-noconfirm** option as this will overwrite data if the URL targets an existing file.

Usage

Backup the current configuration as part of periodic maintenance activities in case of emergencies.

Important: Saving a configuration does not save the boot options as configured via the Global Configuration mode **boot** commands.

Example

The following saves the configuration data to the local file */flash/pub/juneconfig.cfg* with no confirmation from the user:

```
save configuration /flash/pub/juneconfig.cfg -noconfirm
```

The following saves the configuration data to remote host *remoteABC* as */pub/juneconfig.cfg*:

```
save configuration tftp://remoteABC/pub/juneconfig.cfg
```

save logs

Saves the current log file to a local or remote location.

Product

All

Privilege

Security Administrator, Administrator

Syntax

save logs { url } [active] [inactive] [callid *call_id* **] [event-verbosity** *evt_verboseness* **] [facility** *facility* **] [level** *severity_level* **] [pdu-data** *pdu_format* **] [pdu-verbosity** *pdu_verboseness* **] [since** *from_date_time* **[until** *to_date_time* **]] [| { grep** *grep_options* **| more }]**

url

Specifies the location to store the log file(s). *url* may refer to a local or a remote file and must be entered in the following format.
[**file:**] { **/flash** | **/pcmcia1** | **/hd** } [**/***directory*]**/***file_name*
tftp://{ *host*[*:port#*] } [**/***directory*]**/***file_name*
[ftp: | sftp:]//[*username*[*:password*]**@**] { *host* } [*:port#*] [**/***directory*]**/***file_name*

Important: Use of the SMC hard drive is not supported in this release.

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.

Important: *hostname* can only be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserver.

port# is the logical port number that the communication protocol is to use.

active

Saves data from active logs.

inactive

Saves data from inactive logs.

callid *call_id*

Specifies a call ID for which log information is to be saved as a 4-byte hexadecimal number.

event-verbosity *evt_verboseness*

Specifies the level of verboseness to use in displaying of event data as one of:

- *min*: Logs minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.
- *concise*: Logs detailed information about the event, but does not provide the event source within the system.
- *full*: Logs detailed information about event, including source information, identifying where within the system the event was generated.

facility *facility*

Specifies the facility to modify the filtering of logged information. Valid facilities for this command are:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: AAA client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **aal2**: AAL2 protocol logging facility
- **acl-log**: Access Control List logging facility
- **acsctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: Active Charging Service (ACS) Manager facility
- **alarmctrl**: Alarm Controller facility
- **alcap**: ALCAP protocol logging facility
- **alcapmgr**: ALCAPMgr logging facility
- **all**: All facilities
- **asngwmgr**: ASN Gateway Manager facility
- **asnpcmgr**: ASN Paging Controller Manager facility
- **bfd**: BFD protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux-De-mux Manager logging facility
- **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
- **callhome**: Call home application logging facility
- **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)

- **cli**: CLI logging facility
- **credit-control**: Credit Control facility
- **cscf**: IMS/MMD CSCF
- **cscfmgr**: SIP CSCF Manager facility
- **cscfttmgr**: SIP CSCFTT Manager facility
- **csp**: Card Slot Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: Content Service Selection (CSS) RADIUS Signaling facility
- **cx-diameter**: Cx Diameter Messages facility
- **dcardctrl**: IPSEC Daughter Card Controller logging facility
- **dcardmgr**: IPSEC Daughter Card Manager logging facility
- **demuxmgr**: Demux Manager API facility
- **dgmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol logging facility
- **dhcpv6**: DHCPv6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages facility
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting
- **diameter-auth**: Diameter Authentication
- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ACS Diameter signaling facility
- **diameter-hdd**: Diameter HDD Interface facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSEC Data Path facility
- **drvctrl**: Driver Controller facility
- **eap-ipsec**: EAP
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface facility
- **egtpc**: eGTP-C logging facility
- **egtpmgr**: eGTP manager logging facility
- **egtpu**: eGTP-U logging facility
- **epdg**: ePDG logging facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility

- **fng**: FNG logging facility
- **gmm**:
  - For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
  - For 3G: Logs the access application layer (above the RANAP layer)
- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
- **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
- **gss-gcdr**: GTPP Storage Server GCDR facility
- **gtpc**: GTP-C protocol logging facility
- **gtpcmgr**: GTP-C protocol Manager logging facility
- **gtpp**: GTP-PRIME protocol logging facility
- **gtpu**: GTP-U protocol logging facility
- **gtpumgr**: GTPU Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages facility
- **gy-diameter**: Gy Diameter messages facility
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **hdctrl**: HD Controller logging facility
- **hnb-gw**: HNB-GW (3G Femto GW) logging facility
- **hnbmgr**: HNBMGR (3G Femto GW DemuxMgr) logging facility
- **hss-peer-service**: HSS Peer Service facility
- **igmp**: IGMP
- **ikev2**: IKEv2
- **ims-authorizatn**: IMS Authorization Service facility
- **ims-sh**: HSS SH Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **imsue**: IMSUE
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipms**: IPMS logging facility
- **ipsec**: IP Security logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ipsp**: IP Pool Sharing Protocol logging facility
- **kvstore**: KV Store facility
- **l2tp-control**: L2TP control logging facility

- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: LAGMGR logging facility
- **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
- **li**: Refer to the *Lawful Intercept Interface Reference* for a description of this command.
- **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
- **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
- **local-policy**: Local Policy Service facility
- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway manager logging facility
- **map**: MAP Protocol logging facility
- **megadiammgr**: Megadiameter Manager (SLF Service) logging facility
- **mme-app**: Mobility Management Entity Application logging facility
- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: Mobility Management Entity Demux Manager logging facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 logging facility
- **mpls**: MPLS protocol logging facility
- **mseg-app**: MSEG application logging facility
- **mseg-gtpc**: MSEG GTPC application logging facility
- **mseg-gtpu**: MSEG GTPU application logging facility
- **msegmgr**: MSEGMgr (MSEG DemuxMgr) logging facility
- **mtp2**: MTP2 Service logging facility
- **mtp3**: MTP3 Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **npuctrl**: Network Processor Unit Control facility
- **npumgr**: Network Processor Unit Manager facility
- **npumgr-acl**: NPUMGR ACL logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility
- **npumgr-fwd**: NPUMGR FWD logging facility
- **npumgr-init**: NPUMGR INIT logging facility
- **npumgr-port**: NPUMGR PORT logging facility

- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **ntfy-intf**: Notification Interface logging facility
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF protocol logging facility
- **ospfv3**: OSPFv3 protocol logging facility
- **p2p**: Peer-to-Peer Detection logging facility
- **pccmgr**: IPCF PCC Manager library
- **pdg**: PDG logging facility
- **pdgdmgr**: PDG Demux Manager logging facility
- **pdif**: PDIF logging facility
- **pgw**: PDN Gateway logging facility
- **phs**: Payload Header Suppression
- **phs-control**: PHS X1/X5 and X2/X6 Interface logging facility
- **phs-data**: PHS Data logging facility
- **phs-eapol**: PHS EAPOL logging facility
- **phsgwmgr**: PHS Gateway Manager facility
- **phspcmgr**: PHS Paging Controller Manager facility
- **pmm-app**: PMM application logging facility
- **ppp**: PPP link and packet facilities
- **pppoe**: PPPOE logging facility
- **push**: VPNMGR CDR push logging facility
- **radius-acct**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Rf Diameter messages facility
- **rip**: RIP logging facility (RIP is not supported at this time.)
- **rohc**: RObust Header Compression facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RUA (3G Femto GW - RUA messages) logging facility
- **s1ap**: S1AP Protocol logging facility
- **sccp:** SCCP Protocol logging connection-oriented messages between RANAP and TCAP layers.
- **sct**: Shared Configuration Task logging facility

- **sctp**: SCTP Protocol logging facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN 'glue' interfaces, e.g., between PMM, MAP,. GPRS-FSM, SMS.
- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN MBMS Bearer app (SMGR) logging facility
- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSNs System Components logging facility; used infrequently
- **sgsn-test**: SGSN Tests logging facility; used infrequently
- **sgtpcmgr**: SGSN GTPC Manager logging information exchange through SGTPC and the GGSN
- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages facility
- **sitmain**: System Initialization Task main logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
- **sndcp**: SNDCP Protocol logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF SPR Manager logging facility
- **srdb**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **sscfnni**: SSCFNNI Protocol logging facility
- **sscop**: SSCOP Protocol logging facility
- **ssh-ipsec**: SSH IP Security logging facility
- **ssl**: SSL (Secure socket layer messages) logging facility
- **stat**: Statistics logging facility
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **tcap**: TCAP Protocol logging facility
- **testctrl**: Test Controller logging facility
- **testmgr**: Test Manager logging facility
- **threshold**: threshold logging facility

- **ttg**: TTG logging facility
- **tucl**: TUCL logging facility
- **udr**: User detail record facility (used with the Charging Service)
- **user-data**: User data logging facility
- **user-l3tunnel**: User layer-3 tunnel logging facility
- **usertcp-stack**: User TCP Stack
- **vpn**: Virtual Private Network logging facility
- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6

---

level *severity_level*

Specifies the level of information to be logged from the following list which is ordered from highest to lowest:

- *critical*: Logs critical events
- *error*: Logs error events and all events with a higher severity level
- *warning*: Logs warning events and all events with a higher severity level
- *unusual*: Logs unusual events and all events with a higher severity level
- *info*: Logs info events and all events with a higher severity level
- *trace*: Logs trace events and all events with a higher severity level
- *debug*: Logs all events

---

pdu-data *pdu_format*

Specifies output format for the display of packet data units as one of:

- *none* - raw format (unformatted).
- *hex* - hexadecimal format.
- *hex-ascii* - hexadecimal and ASCII similar to a main-frame dump.

---

pdu-verbosity *pdu_verboseness*

Specifies the level of verboseness to use in displaying of packet data units as a value from 1 to 5, where 5 is the most detailed.

---

since *from_date_time* **[until** *to_date_time* **]**

Default: no limit.

since *from_date_time*: Saves only the log information which has been collected more recently than *from_date_time*.

until *to_date_time*: Saves no log information more recent than *to_date_time*. Defaults to current time when omitted.

from_date_time and *to_date_time* must be formatted as YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where:

- YYYY = 4-digit year
- MM = 2-digit month in the range 01 through 12
- DD = 2-digit day in the range 01 through 31

- HH = 2-digit hour in the range 00 through 23
- mm = 2-digit minute in the range 00 through 59
- ss = 2 digit second in the range 00 through 59

to_date_time must be a time which is more recent than *from_date_time*.
Using the **until** keyword allows for a time range of log information; using only the **since** keyword will display all information up to the current time.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in *Command Line Interface Reference*.

Usage

Backup the current log file as part of periodic maintenance activities.

Example

The following saves the log to the local file */flash/pub/junelogs.logs* with no confirmation from the user:

```
save logs /flash/pub/junelogs.logs -noconfirm
```

The following saves the configuration data to remote host *remoteABC* as */pub/junelogs.logs*:

```
save logs tftp://remoteABC/pub/junelogs.logs
```

session trace

Enable or disables the subscriber session trace functionality based on a specified subscriber device or ID on one or all instance of session on a specified UMTS/EPS network element. It also clears/resets the statistics collected for subscriber session trace on a system.

Product

GGSN, MME, P-GW, S-GW

Privilege

Operator

Syntax

session trace { reset statistics | subscriber network-element { mme | pgw | sgw | ggsn } { imei *id* **| imsi** *id* **| interface { all |** *interface* **} } trace-ref** *id* **collection-entity** *ip_address***}**

no session trace subscriber network-element [mme | pgw | sgw | ggsn] [trace-ref *id* **]**

no

Disables the entire session trace or for a specific network element and/or trace reference.

reset statistics

Clears/resets the entire session trace statistical data collected on a system.

Caution: This is a system wide command that affects all statistical data.

session trace subscriber network-element { mme | pgw | sgw | ggsn }

Identifies the network element that, in turn, identifies the interfaces where the session trace is to occur. Specific interfaces can be specified using the interface keyword described below.
ggsn: Specifies that the session trace is to occur on one or all interfaces on the GGSN.
mme: Specifies that the session trace is to occur on one or all interfaces on the MME.
pgw: Specifies that the session trace is to occur on one or all interfaces on the P-GW.
sgw: Specifies that the session trace is to occur on one or all interfaces on the S-GW.

imei *id*

Specifies the International Mobile Equipment Identification number of the subscriber UE. *id* must be the 8-digit TAC (Type Allocation Code) and 6-digit serial number. Only the first 14 digits of the IMEI/IMEISV are used to find the equipment ID.

imsi *id*

Specifies the International Mobile Subscriber Identification (IMSI). *id* must be the 3-digit MCC (Mobile Country Code), 2- or 3- digit MNC (Mobile Network Code), and the MSIN (Mobile Subscriber Identification Number). The total should not exceed 15 digits.

interface { all | *interface* **}**

Specifies the interfaces where the session trace application will collect data.

all: Specifies all interfaces associated with the selected network element
interface: Specifies the interface type where the session trace application will collect trace data. The following interfaces are applicable for the network element type:

- GGSN:
  - **gi**: Specifies that the interface where the trace will be performed is the Gi interface between the GGSN and RADIUS server.
  - **gmb**: Specifies that the interface where the trace will be performed is the Gmb interface between the GGSN and BM-SC.
  - **gn**: Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.
  - **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.
- MME:
  - **s1mme**: Specifies that the interface where the trace will be performed is the S1-MME interface between the MME and the eNodeB.
  - **s3**: Specifies that the interface where the trace will be performed is the S3 interface between the MME and an SGSN.
  - **s6a**: Specifies that the interface where the trace will be performed is the S6a interface between the MME and the HSS.
  - **s10**: Specifies that the interface where the trace will be performed is the S10 interface between the MME and another MME.
  - **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
- P-GW:
  - **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
  - **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
  - **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
  - **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
  - **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
  - **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.
  - **s8b**: Specifies that the interface where the trace will be performed is the S8b interface between the P-GW and the S-GW.
  - **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.
- S-GW:
  - **gxc**: Specifies that the interface where the trace will be performed is the Gxc interface between the S-GW and the PCRF.

- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the S-GW and the MME.
- **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
- **s8b**: Specifies that the interface where the trace will be performed is the S8b interface between the S-GW and the P-GW.

trace-ref *id*

Specifies the trace reference for the trace being initiated. *id* must be the MCC (3 digits), followed by the MNC (3 digits), then the trace ID number (3-byte octet string).

collection-entity *ip_address*

Specifies the IP address of the collection entity where session trace data is pushed in IPv4 dotted-decimal notation.

Usage

Use this command to initiate a session trace for a specified subscriber device or ID on one or all interfaces on a specified network element.

Important: Session trace configuration is performed in the *Global Configuration Mode* using the **session trace** command. Refer to the *Global Configuration Mode Commands* chapter for more information.

Example

The following command initiates a session trace on a P-GW S5 interface for a subscriber with an IMSI of *322233123456789* and sets the trace reference as *322233987654* and the collection entity IP address as *10.2.3.4*:

```
session trace subscriber network-element pgw imsi 322233123456789
interface s5 trace-ref 322233987654 collection-entity 10.2.3.4
```

The following command initiates a session trace on an MME S6a interface for a subscriber with an IMSI of *322233123456789* and sets the trace reference as *322233987654* and the collection entity IP address as *10.2.3.4*:

```
session trace subscriber network-element mme imsi 322233123456789
interface s6a trace-ref 322233987654 collection-entity 10.2.3.4
```

The following command initiates a session trace on a Gn interface on GGSN between GGSN and SGSN for a subscriber with an IMSI of *322233123456789* and sets the trace reference as *322233987654* and the collection entity IP address as *1.2.3.4*:

```
session trace subscriber network-element ggsn imsi 322233123456789
interface gn trace-ref 322233987654 collection-entity 10.2.3.4
```

setup

Enters the system setup wizard which guides the user through a series of questions regarding the system basic configuration options, such as initial context-level administrative users, host name, etc.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
setup
```

Usage

The setup wizard provides a user friendly interface for initial system configuration.

Important: If the configuration script generated by the setup wizard is applied when an existing configuration is in use, the options which are common to both are updated and all remaining options are left unchanged.

Example

```
setup
```

sgs offload

This command starts/stops the marking of subscribers associated with the specified Visitor Location Register (VLR) to an offload state. This enables the MME to preemptively move subscribers away from an MSS which is scheduled to be put in maintenance mode.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

sgs offload sgs-service *sgs_svc_name* **vlr** *vlr_name* **{ start time-duration** *minutes* **| stop } [-noconfirm]**

sgs-service *sgs_svc_name*

Specifies the SGs service to which the VLR belongs.
sgs_svc_name specifies the name for a pre-configured SGs service to associate with the MME service and must be an alphanumeric string of 1 through 63 characters. For more information on the SGs service, refer to the **sgs-service** command in the *Context Configuration Mode Commands* chapter and refer to the *MME SGs Service Configuration Mode Commands* chapter.

vlr *vlr_name*

Specifies the VLR service which should be marked in an offload state.
vlr_name specifies the name for a pre-configured VLR to associate with the SGs service and must be an alphanumeric string of 1 through 63 characters. For more information, refer to the **vlr** command in the *MME SGs Service Configuration Mode Commands* chapter.

start time-duration *minutes*

Specifies that the offload state should be set for the specified the VLR.
time-duration defines the period in *minutes* over which all qualifying subscribers will be marked in offload state. For example, a setting of 40 minutes with 40000 subscribers will result in a release rate of 1000 per minute. *minutes* must be an integer from 1 to 1000.
Note: While the **time-duration** value is not used in Release 12.2 or earlier, it is required for completion of the **start** command.

stop

Specifies that the offload state should no longer be set for the specified the VLR.

-noconfirm

Indicates that the command is to execute without additional prompt and confirmation from the user.

Usage

When this offload command is set on the MME, all sessions matching this VLR are marked with an ‘offload’ flag. During the next UE activity, the MME requires each UE to perform a combined TAU/LAU.

When issuing the command to place a VLR in an offload state, the MME notifies the operator if this is the last available VLR in a pool.
More than one VLR may be offloaded at the same time.
Related Commands:

- To display VLR offload information and statistics for a specified SGs service name, refer to the **show sgs-service offload service-name** *sgs_svc_name* command.

Example

The following command starts marking the subscribers associated with *vlr1* for offload.

```
sgs offload sgs-service sgs1 vlr vlr1 start time-duration 60 -noconfirm
```

sgsn clear-detached-subscriptions

Clears subscription data belonging to a subscriber who has already detached.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
sgsn clear-detached-subscriptions imsi imsi
```

imsi *imsi*

Specifies the international mobile subscriber identity (IMSI) of the subscriber session identifying the subscription data to be cleared.

Usage

This command can be issued on either a 2G or 3G SGSN to clear subscription data (including subscription information, and information for P-TMSI allocated, received authorization vectors, and NGAF flag values). This command is only effective if the subscriber has already detached.
After the data is purged, the SGSN sends an appropriate message to the HLR.
Related Commands:

- To clear subscription data for subscribers that are currently attached, refer to the **admin-disconnect-behavior clear-subscription** commands described in the chapters for *GPRS Service Configuration Mode* or the *SGSN Service Configuration Mode*.

Example

```
sgsn clear-detached-subscriptions imsi 040501414199978
```

sgsn imsimgr

Initiates an audit for managing the SGSN's IMSI manager's (IMSIMgr) IMSI table.

Important: These commands are used primarily for troubleshooting purposes and are intended for the use of specially trained service representatives.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sgsn imsimgr { add-record *imsi* **sessmgr instance** *sessmgr#* **| audit-with sessmgr { all | instance** *sessmgr#* **} | remove-record** *imsi* **}**

add-record *imsi*

Adds a record for an IMSI to the IMSI manager's table and associates a specific session manager (SessMgr) with the IMSI.
imsi: Enter up to 15 digits. An IMSI consists of the 3-digit MCC (mobile country code) + the 2- or 3-digit MNC (mobile network code) + the MSIN (mobile station identification number) for the remaining 10 or 9 digits (depending on the length of the MNC).

sessmgr instance *sessmgr#*

Specifies a Session Manager (SessMgr) instance associated with the IMSI as an integer from 0 through 4095.

audit-with sessmgr { all | instance *sessmgr#* **}**

Initiates an IMSI audit with all SessMgrs or a Session Manager (SessMgr) instance specified as an integer from 0 to 4095.

remove-record *imsi*

Deletes a specific IMSI from the IMSI table.
imsi: Enter up to 15 digits. An IMSI consists of the 3-digit MCC (mobile country code) + the 2- or 3-digit MNC (mobile network code) + the MSIN (mobile station identification number) for the remaining 10 or 9 digits (depending on the length of the MNC).

Usage

Use this command to manage the IMSIMgr's IMSI table, and to initiate an audit of one or more SessMgrs with the IMSIMgr so that the IMSI table has the correct IMSI-SessMgr association. After this audit, any IMSI in the IMSIMGR which is not found in any Sessmgr is deleted and similarly any missing entries at the IMSIMgr are created.

Example

Delete IMSI *044133255524211* from the audit table:

```
sgsn imsimgr remove-record 044133255524211
```

sgsn offload

Instructs the SGSN to begin the offloading procedure and actually starts and stops the offloading of subscribers which is part of the SGSN Gb (2G) or Iu (3G) Flex load redistribution functionality.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sgsn offload [gprs-service *srvc_name* **| sgsn-service** *srvc_name* **}** *srvc_name* **{ activating [nri-value** *nri_value* **| stop nri-value** *nri_value* **] | connecting [nri-value** *nri_value* **| stop [nri-value** *nri_value* **| target-nri** *target_nri* **target-count** *target_count* **] | t3312-timeout** *seconds* **| target-nri** *target_nri* **target-count** *target_count* **] }**

gprs-service *srvc_name*

Specifies a unique alphanumeric string of 1 through 63 characters that identifies a GPRS service that has already been defined for the 2G SGSN configuration.

sgsn-service *srvc_name*

Specifies a unique alphanumeric string of 1 through 63 characters that identifies an SGSN service that has already been defined for the 3G SGSN configuration.

activating

Instructs the SGSN to off load any subscribers sending an “activate request” message.

connecting

Instructs the SGSN to off load any subscribers sending either an “attach request” or a “RAU request” message.

nri-value *nri-value*

Sets the local NRI. Including this keyword in the configuration instructs the SGSN to check the P-TMSI and use the SGSN matching the configured NRI value to off load subscribers.

Important: **nri-value** and **target-nri** are mutually exclusive.

nri-value is an integer from 1 through 63 that identifies a specific, already defined, SGSN in a pool. (NRI defined in the service configuration.)
Use of 0 (zero) value is not recommended.

stop

Instructs the SGSN to stop offloading subscribers from the pool area.

target-nri *target_nri*

Instructs the SGSN to begin dynamically load balancing across a network of pooled SGSNs.
target_nri is an integer from 0 through 63 that identifies an already defined target NRI (SGSN) to which the subscribers are to be offloaded. (NRI previously defined in the service configuration.)
Use of 0 (zero) value is not recommended.

target-count *target_count*

Identifies the number of subscribers to be offloaded as an integer from 0 through 4000000.

t3312-timeout *seconds*

Configures the timer (in seconds) for sending period RAUs to the MS as an integer from 2 through 60.
Default: 4

Usage

Use this command to configure the offloading of subscribers which is a part of the SGSN's load redistribution operation. This command can be used anytime an SGSN is to be taken out of service. Commands, with different NRI values, are repeated to expand/contract the radius of the offloading.
When targeted offloading is to be used, you should choose an algorithm to control offloading from the perspective of the IMSIMGR and SESSMGR. This is done with the **target-offloading** command in the SGSN-Global configuration mode.

Example

Command 1: The following command instructs the SGSN to begin offloading for the local NRI id *1* in the *gprs1* GPRS service configuration:

```
sgsn offload gprs-service gprs1 connecting nri-value 1
```

Command 2: Enter this second command to add offloading for NRI *2* to the offloading already occurring for NRI *1*:

```
sgsn offload gprs-service gprs1 connecting nri-value 2
```

Command 1: The following command instructs the SGSN to begin offloading for all local NRIs to the target NRIs *5* and *6* for *100000* and *200000* subscribers respectively:

```
sgsn offload sgsn-service sgsnserv4 connecting target-nri 5 target-count
100000 target-nri 6 target-count 200000
```

Command 2: The following command instructs the SGSN to add target NRI *4* to the offloading and also to change the subscriber offload number for target NRI *5*:

```
sgsn offload sgsn-service sgsnserv4 connecting target-nri 4 target-count
100000 target-nri 5 target-count 300000
```

sgsn op

Instructs the SGSN to begin specific operations or functions.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sgsn op { auth-ptmsi-counters imsi *imsi* **| convert | nse { fr | ip | sgsn-invoke-trace } | show | ss7-rd** *ss7-rd_id* **{ destination | link | linkset | peer } }**

---

auth-ptmsi-counters imsi *imsi*

Displays the authentication, P-TMSI reallocation, and P-TMSI signature reallocation counters for the specified IMSI.
imsi: Enter a unique 15-digit number associated with a mobile phone.

---

convert point-code *pt_code* **variant** *variant*

Converts SS7 point codes, according to identified variants, from dotted-decimal format to decimal format and vice versa.
point-code *pt_code*: Enters an SS7 point code in either dotted-decimal format or decimal format.
variant *variant*: Identifies the appropriate variant for the point code:

- **ansi**
- **itu**
- **ttc**

---

nse { fr *operation* **| ip** *operation* **| sgsn-invoke-trace nse-id** *nse_id* **}**

Enables the operator to perform a range of live control functions (for example, reset, block, unblock) for various types of virtual connections based on the signalling type of the NSE:
fr: Identifies a Frame Relay NSE.
ip: Identifies an IP NSE.
operation: Identifies the operation to be performed for the NSE connection (if available for the selected signalling type):

- **block nse-id** *nse_id*: Blocks signal flow through all network service virtual connections (NSVC) for the specified NSE:
  - *nse_id*: an integer from 0 to 65535.
- **bvc-flc-limit rate** *rate* **bvc-id** *bvc_id* **nse-id** *nse_id* - SGSN initiates flow control at the defined percentage rate to limit the flow through the BSSGP virtual connection (BVC) for the specified NSE and optionally for a specified BVC.
  - *rate*: an integer from 0 to 100.
  - *bvc_id*: an integer from 0 to 65000.
  - *nse_id*: an integer from 0 to 65535.
- **bvc-reset bvc-id** *bvc_id* **nse-id** *nse_id*: SGSN initiates a BVC-Reset on the specified BVC and NSE:

- *bvc_id*: an integer from 0 through 65000.
- *nse_id*: an integer from 0 through 65535.

- **nsvc** *nsvc_id* **{ block | enable | disable | unblock }***nse_id* - SGSN initiates NS-Block or NS-Unblock for the specified NSVC of the specified NSE:
  - *nsvc_id*: an integer from 0 through 65535.
  - *nse_id*: an integer from 0 through 65535.
- **reset nse-id** *nse_id* - SGSN initiates NS-Reset for all NSVC configured in the NSE. *nse_id* is an integer from 0 through 65535.
- **unblock nse-id** *nse_id* - SGSN initiates NS-Unblock for all NSVC configured for the specified NSE. *nse_id* is an integer from 0 through 65535.

sgsn-invoke-trace nse-id *nse_id* **record-type** *record_type* **trace-reference** *reference* **[mobile-id type** *id_type* **| trace-transaction-id** *trace_id* **]** :

Important: This command can be used for troubleshooting/debugging purposes and is primarily intended for the use of specially trained service representatives.

Instructs the SGSN (1) to send the BSSGP message SGSN-INVOKE-TRACE to the BSC to initiate a BSC trace of a particular MS and (2) to define the type and triggering of the trace.

- *nse_id*: Identifies the peer NSE, enter an integer from 0 to 65535.
- *record_type*: Specifies the type of trace to be performed:
  - **basic**
  - **handover**
  - **no-bss-trace**
  - **radio**
- **trace-reference** *reference* : Specifies the trace reference ID as an integer from 0 to 65535.
- **mobile-id type** *id_type*: Select the appropriate mobile ID type for the MS that is to be traced:
  - **imei value** *value* - Specifies the mobile ID type as the unique International Mobile Equipment Identity.

    value: 15-digit IMEI value.
  - **imeisv value** *value*: Specifies the mobile ID type as the unique International Mobile Equipment Identity with the two-digit software version number.

    value: 16-digit IMEISV value.
  - **imsi value** *value* - Specifies the mobile ID type as a network unique International Mobile Subscriber Identity as a 15-digit IMSI value.
- **trace-transaction-id** *trace_id*: Specifies the trace transaction ID as an integer from 0 through 65535.

show plmn-list smgr-inst *sessmgr#*

Important: This function is only available in release 8.1.

SGSN displays the configured PLMN list for the specified session manager (SessMgr):

sessmgr#: Enter up to 4 digits, 0 to 4095.

---

ss7-rd *ss7-rd_id* **{ destination | link | linkset | peer }**

The **ss7-rd** commands assist with troubleshooting connections between the SGSN and the peer server.
ss7-rd_id: Specifies the configured SS7 routing domain as an integer from 1 through 12.

- **destination audit asp-instance** *asp_id* **peer-server-id** *peer_id* **psp-instance-id** *psp_id*

  Initiates destination audit (DAUD) messages for all point codes reachable via the identified peer-server, which is in restricted/unavailable/congested state due to DRST/DUNA/SCON messages respectively from the far end.

  - *asp_id*: Specifies the relevant ASP configuration ID as an integer from 1 through 4.
  - *peer_id*: Specifies the relevant peer server configuration ID as an integer from 1 through 144.
  - *psp_id*: Specifies the relevant PSP configuration ID as an integer from 1 through 4

- **link** *procedure* **linkset-id** *linkset_id* **link-id** *link_id*

  Initiates MTP3 network link management procedures for the specified link:

  - **activate**: Activates the deactivated link.
  - **deactivate**: Deactivates specified link.
  - **deactivate-l2-only**: Deactivates the link only at the MTP3 layer.
  - **inhibit**: Inhibits the link only if it does *not* make any destination unreachable.
  - **uninhibit**: Uninhibits the inhibited link.
  - *linkset_id*: an integer between 1 and 144.
  - *link_id*: an integer between 1 and 16.

- **linkset-id** *procedure* **linkset-id** *linkset_id*

  Initiates MTP3 network link management procedures for all the links in the specified linkset:

  - **activate**: Activates the deactivated linkset.
  - **deactivate**: Deactivates the linkset.
  - **deactivate-l2-only**: Deactivates the linkset only at MTP3 layer.
  - *linkset_id*: an integer between 1 and 144.

- **peer** *message* **asp-instance** *asp_id* **peer-server-id** *peer_id* **psp-instance-id** *psp_id*

  Initiates one of the following SCTP/M3UA management messages from the identified link:

  - **abort**: Sends an SCTP Abort message which aborts the SCTP association ungracefully.
  - **activate**: Sends an M3UA ASP Active message to activate the link.
  - **down**: Sends an M3UA ASP Down message to bring down the M3UA link.
  - **establish**: Sends an SCTP INIT message to start the SCTP association establishment.
  - **inactivate**: Sends an M3UA ASP Inactive message to deactivate the link.
  - **inhibit**: Inhibits the M3UA link locally when the operator wants to lockout the link.
  - **terminate**: Sends SCTP Shutdown message which closes the SCTP association gracefully.
  - **un-inhibit**: Uninhibits the M3UA link.
  - **up**: Sends an M3UA ASP UP message to bring up the M3UA link.
  - *asp_id*: Specifies a relevant ASP configuration ID as an integer from 1 through 4.

- *peer_id*: Specifies the relevant peer server configuration ID as an integer from 1 through 144.
- *psp_id*: Specifies the relevant PSP configuration ID as an integer from 1 through 4

Usage

In most cases, an operator will block/unblock/reset from the BSC-side. The **nse** commands cause the SGSN to initiate actions, usually for one of the following reasons:

- to resolve issues on the BSC-side,
- as part of an upgrade to the BSC,
- as part of link expansion,
- to resolve NSVC/BVC status mismatches observed between the SGSN and BSC.

The **sgsn-invoke-trace** command initiates the trace procedure where the BSC begins a trace record on a specified MS.

Example

The following command instructs the SGSN to initiate an NS-Block for all NSVC associated with Frame Relay NSE ID *2422*:

```
sgsn op nse fr unblock nse-id 2422
```

Activate linkset *1* configured in SS7 routing domain *1*:

```
sgsn op ss7-rd 1 linkset activate linkset-id 1
```

sgsn retry-unavailable-ggsn

Marks the GGSN as available for further activation.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sgsn retry-unavailable-ggsn *ip_address*

ip_address

Specifies the IP address of a GGSN in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

This command allows the operator to directly inform both the session manager and the SGTPC manager that the GGSN has been removed from a blacklist and is now available for activations. This action would override the GGSN blacklist timer configuration with **ggsn-fail-retry-timer** in the SGTP service configuration mode.

Example

The following command indicates that the GGSN identified by its IP address is now available for activation:

```
sgsn retry-unavailable-ggsn 198.168.128.8
```

sgtpc test echo sgsn-address

Initiates SGTPC echo test procedure.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sgtpc test echo sgsn-address *sgsn_ip_address* **{ all | ggsn-address** *ggsn_ip_address* **}**

sgsn-address *sgsn_ip_address*

Identifies the IP address of the SGSN issuing the test in IPv4 dotted-decimal notation.

all

Sends GTPC echo requests to all GGSNs having current sessions with the SGTP service.

ggsn-address *ggsn_ip_address*

Sends a GTPC echo request to the specified GGSN whether or not the GGSN has active sessions with the SGTP service. *ggsn_ip_address*is entered using IPv4 dotted-decimal notation.

Usage

This command initiates a test for the GTPC echo procedure -- echo from the specified SGSN to a specified GGSN or to all GGSNs that have sessions with the SGTP service. Issue the command from the Exec Mode within the context in which the SGTP service is configured.
Note that if the GGSN does not respond to the initial echo request, the echo requests will be retried for the max-retransmissions times.

Example

This SGSN with IP address of *10.1.1.1* sends an echo test to all GGSNs attached to the SGTP service:

```
sgtpc test echo sgsn-address 10.1.1.1 all
```

shutdown

Terminates all processes within the chassis. After all processes are terminated, the system initiates a hardware reset (reboot). This command is identical to the **reload** command.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
shutdown [ -noconfirm ]
```

-noconfirm

Executes the command without any additional prompts or confirmation from the user.

Usage

The system performs a hardware reset and reloads the highest priority boot image and configuration file specified in the boot.sys file. Refer to the **boot system priority** command in the Global Configuration Mode for additional information on configuring boot images, configuration files and priorities.

Important: To avoid the abrupt termination of subscriber sessions, it is recommended that a new call policy be configured and executed prior to invoking the **shutdown** command. This policy sets busy-out conditions for the system and allows active sessions to terminate gracefully. Refer to the **newcall** command in the Exec Mode for additional information.

Caution: Issuing this command causes the system to become unavailable for session processing until the reboot process is complete.

Example

The following command performs a hardware reset on the system:

```
shutdown
```

sleep

Pauses the command line interface (CLI).

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

sleep *seconds*

sleep *seconds*

Specifies the number of seconds to pause as an integer from 1 through 3600.

Usage

Sleep is a command delay which is only useful when creating command line interface scripts such as predefined configuration files/scripts.

Example

The following will cause the CLI to pause for *30* seconds.

```
sleep 30
```

srp initiate-switchover

Changes the device status on the primary and backup systems configured for Interchassis Session Recovery (ICSR) support employing Service Redundancy Protocol (SRP).

Product

All products that support ICSR

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

srp initiate-switchover [post-processing-timeout | reset-route-modifier | timeout *seconds* **] [-noconfirm]**

post-processing-timeout

Specifies the timeout value (in seconds) to initiate the post-switchover process as an integer from 0 through 3600.

reset-route-modifier

During a switchover, resets the route-modifier to the initial value.

timeout *seconds*

Specifies the number of seconds before a forced switchover occurs as an integer from 0 through 65535. Default: 300

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

This command executes a forced switchover from active to inactive. The command must be executed on the active system and switches the active system to the inactive state and the inactive system to an active state.

Example

The following initiates a switchover in *30* seconds.

```
srp initiate-switchover timeout 30
```

srp reset-auth-probe-fail

Resets Service Redundancy Protocol (SRP) authentication probe monitor failure information.

Product

All products that support Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
srp reset-auth-probe-fail
```

Usage

This command resets the auth probe monitor failure information to 0.

srp reset-diameter-fail

Resets Service Redundancy Protocol (SRP) Diameter monitor failure information.

Product

All products that support Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
srp reset-diameter-fail
```

Usage

This command resets the Diameter monitor failure information to 0.

srp terminate-post-process

forcibly terminates post-switchover processing by primary and backup systems configured for Interchassis Session Recovery (ICSR) support employing Service Redundancy Protocol (SRP).

Product

All products that support ICSR

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
srp terminate-post-process [ -noconfirm ]
```

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to force the termination of post-switchover process.

Example

```
srp terminate-post-process
```

srp validate-configuration

Initiates a configuration validation check from the active chassis via Service Redundancy Protocol (SRP).

Product

All products that support Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Syntax

```
srp validate-configuration
```

Usage

Validates the configuration for an active chassis.

srp validate-switchover

Validates both active and standby systems are ready for a planned Service Redundancy Protocol (SRP) switchover.

Product

All products that support Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Syntax

```
srp validate-switchover
```

Usage

Validates that both active and standby systems are ready for a planned SRP switchover.

ssh

Connects to a remote host using a secure shell (SSH) interface.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

ssh { *host_name* | *host_ip_address* } [port *port_num*] [user *user_name*]

host_name | *host_ip_address*

Identifies the remote node with which to attempt connection.
host_name: specifies the remote node using its logical host name which must be resolved via DNS lookup.
host_ip_address: specifies the remote node using its assigned IP address in IPv4 dotted-decimal notation.

port *port_num*

Specifies a specific port for connection as an integer from 1025 through 10000.

user *user_name*

Specifies the user name attempting connection.

Usage

SSH connects to a remote network element using a secure interface.

Example

The following connects to remote host *remoteABC* as user *user1*.

```
ssh remoteABC user user1
```

The following connects to remote host *10.2.3.4* without any default user.

```
ssh 10.2.3.4
```

The following connects to remote host *10.2.3.4* via port *2047* without any default user.

```
ssh 10.2.3.4 port 2047
```

start crypto security-association

Initiates Internet Key Exchange (IKE) negotiations.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

start crypto security-association *cryptomap*

cryptomap

Specifies the name of an existing crypto map policy to use when starting the IKE negotiations as an alphanumeric string of 1 through 127 characters.

Usage

Use this command to start IKE negotiations for IPSEC.

Example

The following command starts the IKE negotiations using the parameters set in the crypto map named *crytpomap1*:

```
start crypto security-association cryptomap1
```

system

Configures information about the system that will be accessible by the SNMP agent.

Product

P-GW

Privilege

Security Administrator, Administrator

Syntax

```
system { carrier-id mcc mcc_num mnc mnc_num | contact name | description description |
hostname name | location location }

default system { contact | description | hostname | location }

no system carrier-id
```

carrier-id mcc *mcc_num* **mnc** *mnc_num*

Specifies the system's Carrier ID via the three-digit MCC (mobile country code) and three-digit MNC (mobile network code).

contact *name*

Specifies the system's contact name as an alphanumeric string from 0 through 255 characters.

description *description*

Defines description text that as an alphanumeric string from 1 through 255 characters that includes text and some parameters, including:

- **%version%** - software version
- **%build%** - software build number
- **%chassis%** - chassis type ("asr5000")
- **%staros%** - ID of the kernel revision
- **%ostype%** - os type
- **%hostname%** - system name
- **%release%** - release
- **%kerver%** - kernel version
- **%machine%** - machine hardware name

Default: "%ostype% %hostname% %release% %kerver% %machine%"
After replacing the parameters with values, the string will be truncated if the length is greater than 255.

hostname *name*

Specifies the system's host name (name of system) as an alphanumeric string of 1 through 63 characters.

location *location*

Specifies the system's geographic or referenced location as an alphanumeric string of 0 through 255 characters.

default system { contact | description | hostname | location }

Sets/restores the default value assigned for specified parameter.

no system carrier-id

Removes the Carrier ID established for the system.

Usage

Use this command to configure information about the system that is accessible by the SNMP agent.

Example

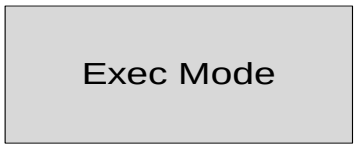
The following command identifies the system's location as *boston*:

```
system location boston
```

Chapter 113
Exec Mode (T-Z)

This section includes the commands **`telnet`** through **`upgrade url-blacklisting database`**.

The Exec Mode is the initial entry point into the command line interface system. Exec mode commands are useful in troubleshooting and basic system monitoring.



telnet

Connects to a remote host using the terminal-remote host protocol.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

telnet { *host_name* | *host_ip_address* } [port *port_num*]

host_name | *host_ip_address*

Identifies the remote node with which to attempt connection.
host_name: specifies the remote node using its logical host name which must be resolved via DNS lookup.
host_ip_address: specifies the remote node using its assigned IP address entered using the IPv4 dotted-decimal notation.

port *port_num*

Specifies a specific port for connect connection as an integer from 1025 through 10000.

Usage

Telnet to a remote node for maintenance activities and/or troubleshooting when unable to do so directly.

Important: **telnet** is not a secure method of connecting between two hosts. **ssh** should be used whenever possible for security reasons.

Example

The following connects to remote host *remoteABC*.

```
telnet remoteABC
```

The following connects to remote host *10.2.3.4* port *2047*.

```
telnet 10.2.3.4 port 2047
```

terminal

Sets the number of rows or columns for display output.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

terminal { length *lines* **| width** *characters* **}**

length *lines* **| width** *characters*

length *lines*: sets the terminal length in number of lines (rows) of text from 5 to 4294967295 lines or the special value of 0 (zero). The value 0 sets the terminal length to infinity.
width *characters*: sets the terminal width in number of characters from 5 to 512 characters.

Usage

Set the length to 0 (infinite) when collecting the output of a command line interface session which is part of a scripted interface.

Example

The following sets the length then width in two commands.

```
terminal length 66

terminal width 160
```

The following command sets the number of rows of the terminal to infinity.

```
terminal length 0
```

test alarm

Tests the alarm capabilities of the chassis.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
test alarm { audible | central-office { critical | major | minor } }
```

audible | central-office { critical | major | minor }

audible: Tests the internal alarm on the System Management Card (SMC) for 10 seconds. The alarm status is returned to its prior state, such as if the audible alarm was enabled prior to the test, the alarm will again be enabled following the test.
central-office { **critical** | **major** | **minor** }: Tests the specified central office alarm type.

Usage

Test the alarm capabilities of the chassis as periodic maintenance to verify the hardware for generation of the internal audible alarms is functional.

Caution: The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

Example

```
test alarm audible

test alarm central-office critical

test alarm central-office major

test alarm central-office minor
```

test ipcf bindmux

Tests the status of the IPCF BindMux Manager instance and also starts or stops the BindMux Manager instance on the chassis.

Product

IPCF

Privilege

Security Administrator, Administrator, Operator

Syntax

```
test ipcf bindmux [ start | stop ]
```

start

Starts the IPCF BindMux Manager on the chassis. If already an instance of IPCF BindMux Manager is running it prompts accordingly.

stop

Stops the IPCF BindMux Manager instance running on the chassis.

Usage

Use this command to test the status of IPCF BindMux Manager instance and also to start or stop the BindMux Manager instance on the chassis.

Caution: The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

Example

The following command stops the BindMux Manager instance running on the chassis:

```
test ipcf bindmux stop
```

test ipsec tunnel

Tests a specified IPSec tunnel.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

test ipsec tunnel { ip pool | *pool_name* destination-ip *ip_address* }

ip pool *pool_name* **destination-ip** *ip_address*

ip pool *pool_name*: Specifies the name of an existing IP pool as an alphanumeric string of 1 through 32 characters.
destination-ip *ip_address*: Specifies a destination IP address in IPv4 dotted-decimal or IPv6 colon-separated notation

Usage

Use this command to test a specified IPSec tunnel.

Caution: The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

Example

```
test ipsec tunnel ip pool pool3 destination-ip 10.2.3.4
```

test mobile tunnel

Tests for the existence of a specified mobile tunnel.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

test mobile tunnel { callid *call_id* **| imsi** *imsi_value* **| ipaddr** *ip_address* **| msid** *msid_num* **| nai** *nai_value* **}**

callid *call_id*

Specifies the exact call instance ID which is to have trace data logged.as a 4-byte hexadecimal number.

imsi *imsi_value*

Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session to be monitored an integer from 1 though 15 characters.

ipaddr *ip_address*

Specifies the IP address of the subscriber session to be monitored in IPv4 dotted-decimal or IPv6 colon-separated notation.

msid *msid_num*

Specifies the mobile subscriber identification number to be monitored as 7 to 16 digits of an IMSI, MIN, or RMI.

nai *nai_value*

Specifies the mobile session Network Access Identifier as an alphanumeric string of 1 through 256 characters. The NAI is the user identity submitted by the client during network access authentication.

Usage

Use this command to test a specified mobile tunnel.

Caution: The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

Example

```
test mobile tunnel ipaddr 192.64.66.9
```

timestamps

Enables or disables the generation of a timestamp in response to each command entered. The timestamp does not appear in any logs as it is a CLI output only. This command affects the current CLI session only. Use the **timestamps** command in the Global Configuration Mode to change the behavior for all future CLI sessions.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
[ no ] timestamps
```

no

Disables generation of timestamp output for each command entered. When omitted, the output of a timestamp for each entered command is enabled.

Usage

Enable timestamps when logging a CLI session on a remote terminal such that each command will have a line of text indicating the time when the command was entered.

traceroute

Collects information on the route data will take to a specified host.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Important: Inspector privileges are granted for all variables except **count and port**. To initiate a traceroute count or to target a specific port for a traceroute, you must have a minimum privilege level of Operator.

Syntax

traceroute { *host_name* | *host_ip_address* } [**count** *packets*] [**df**] [**maxttl** *max_ttl*] [**minttl** *min_ttl*] [**port** *port_num*] [**size** *octet_count*] [**src** { *src_host_name* | *src_host_ip_address* }] [**timeout** *seconds*] [| { **grep** *grep_options* | **more** }]

host_name | *host_ip_address*

Identifies the remote node to trace the route to.
host_name: specifies the remote node using its logical host name which must be resolved via DNS lookup.
host_ip_address: specifies the remote node using its assigned IP address entered using the IPv4 dotted-decimal notation.

count *packets*

Specifies the number of UDP probe packets to send. Default: 3

df

Indicates the packets for the tracing of the route should not be fragmented. If a packet requires fragmenting, it is dropped and the result is the ICMP response “Unreachable, Needs Fragmentation” is received.

maxttl *max_ttl*

Specifies the maximum time to live for the route tracing packets as an integer from 1 through 255. *max_ttl* must be greater than *min_ttl* whether *min_ttl* is specified or defaulted. Default: 30
The time to live (TTL) is the number of hops through the network; it is not a measure of time.

minttl *min_ttl*

Specifies the minimum time to live for the route tracing packets as an integer from 1 through 255. *min_ttl* must be less than *max_ttl* whether *max_ttl* is specified or defaulted. Default: 1
The time to live (TTL) is the number of hops through the network; it is not a measure of time.

port *port_num*

Specifies a specific port for connection as an integer from 1 through 65535. Default: 33434

size *octet_count*

Specifies the number of bytes for each packet as an integer from 40 through 32768. Default: 40

src { *src_host_name* | *src_host_ip_address* }

Specifies an IP address to use in the packets as the source node. Default: originating system's IP address
src_host_name: specifies the remote node using its logical host name which must be resolved via a DNS lookup.
src_host_ip_address: specifies the remote node using its assigned IP address specified entered using IPv4 dotted-decimal notation.

timeout *seconds*

Specifies the maximum time (in seconds) to wait for a response from each route tracing packet as an integer from 2 through 100. Default: 5

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in this guide.

Usage

Trace an IP route when troubleshooting network problems where certain nodes are having significant packet delays or packet loss. This can also be used to identify bottlenecks in the routing of data within the network.

Example

The following command traces the route to remote host *remoteABC* and sends the output to the more command.

```
traceroute remoteABC | more
```

The following command traces the route to remote host *10.2.3.4*'s port *2047* waiting a maximum of *2* seconds for responses.

```
traceroute 10.2.3.4 port 2047 timeout 2
```

update active-charging

Updates specified active charging option(s) for the matching sessions.

Product

ACS, FW, NAT, TPO

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

update active-charging { switch-to-fw-and-nat-policy *fw_nat_policy_name* **| switch-to-rulebase** *rulebase_name* **| switch-to-tpo-policy** *tpo_policy_name* **} { all | callid** *call_id* **| fw-and-nat-policy** *fw_nat_policy_name* **| imsi** *imsi* **| ip-address** *ip_address* **| msid** *msid* **| rulebase** *rulebase_name* **| tpo-policy** *tpo_policy_name* **| username** *user_name* **} [-noconfirm] [| { grep** *grep_options* **| more }]**

switch-to-fw-and-nat-policy *fw_nat_policy_name*

Specifies an existing Firewall-and-NAT policy to switch to as an alphanumeric string of 1 through 63 characters.

switch-to-rulebase *rulebase_name*

Specifies an existing rulebase to switch to as an alphanumeric string of 1 through 63 characters.

switch-to-tpo-policy *tpo_policy_name*

Specifies an existing TPO policy to switch to as an alphanumeric string of 1 through 63 characters.

all

Updates rulebase/policy for all subscribers.

callid *call_id*

Updates rulebase/policy for the Call Identification number specified as an eight-digit hexadecimal number.

fw-and-nat-policy *fw_nat_policy_name*

Updates the rulebase/policy for sessions matching an existing Firewall-and-NAT policy specified as an alphanumeric string of 1 through 63 characters.

imsi *imsi*

Updates rulebase/policy for International Mobile Subscriber Identification (IMSI) specified here. *imsi* must be 3 digits of MCC (Mobile Country Code), 2 or 3 digits of MNC (Mobile Network Code), and the rest with MSIN (Mobile Subscriber Identification Number). The total should not exceed 15 digits. For example, 123-45-678910234 can be entered as 12345678910234.

ip-address *iP_address*

Updates rulebase/policy for the IP address specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

msid *msid*

Updates rulebase/policy for an MSID specified as a string of 1 through 24 characters.

rulebase *rulebase_name*

Updates rulebase/policy for sessions matching an existing rulebase specified as an alphanumeric string of 1 through 63 characters.

tpo-policy *tpo_policy_name*

Updates rulebase/policy for sessions matching an existing TPO policy specified as an alphanumeric string of 1 through 63 characters.

username *user_name*

Updates rulebase/policy for user specified as a an alphanumeric of characters and/or wildcard characters ('$' and '*') of 1 through 127 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the Regulating a Command's Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Use this command to change specified active charging option(s) for the matching sessions.

Example

The following command changes the rulebase for sessions using the rulebase named *standard* to use the rulebase named *super*:

```
update active-charging switch-to-rulebase super rulebase standard
```

update cscf

Causes a NOTIFY to be triggered from CSCF based on registration state and event and indicating the expiry timer value for each contact as “reauthentication-time” provided from the CLI. The subscriber is supposed to send a fresh REGISTER message within “reauthentication-time”, which will be challenged by CSCF as part of reauthentication. If reauthentication fails, the subscriber will be cleared after “reauthentication-time”.

Product

SCM (P-CSCF, S-CSCF)

Privilege

Administrator

Syntax

update cscf subscriber { all | username *user_name* **} cscf-service** *service_name* **{ { [contact** *contact_address* **] reg-state { active event { refreshed | shortened } time** *sec* **} | terminated event { deactivated | expired | rejected | unregistered } } | reauthentication-time** *sec* **} [verbose]**

---

subscriber { all | username *user_name* **}**

Updates CSCF subscriber data.
all: Updates data for all subscribers within a specified CSCF service.
username *user_name*: Specifies the name of a user within the current context as an alphanumeric string of 1 through 127 characters that is case sensitive.

---

cscf-service *service_name*

Specifies a configured CSCF service as an alphanumeric string of 1 and 63 characters that is case sensitive.

---

contact *contact_address*

Specifies the contact address of the subscriber as an alphanumeric string of 1 through 255 characters.

---

reg-state

Specifies the registration state of the subscriber.

---

active event { refreshed | shortened } time *sec* **}**

Specifies the registration state active event type.

- **refreshed**: Specifies registration state active event as refreshed.
- **shortened**: Specifies registration state active event as shortened.

time *sec*: Specifies the time (in seconds) within which subscriber is expected to re-authenticate as an integer from 1 to 86400.

---

terminated event { deactivated | expired | rejected | unregistered }

Specifies the registration state terminated event type.
deactivated: Specifies registration state terminated event as deactivated.
expired: Specifies registration state terminated event as expired.
rejected: Specifies registration state terminated event as rejected.
unregistered: Specifies registration state terminated event as unregistered.

reauthentication-time *sec*

Specifies the time (in seconds) within which the subscriber is expected to re-authenticate as an integer from 1 to 86400.

verbose

Show detailed information.

Usage

This command is only applicable for a P-CSCF and S-CSCF service. When optional contact ID is not specified, all the contact IDs associated with specified user or all users will be updated and trigger NOTIFY.

Important: reauthentication-time should be greater than the current expiry time of the contact so that CSCF will initiate the NOTIFY message.

Example

The following command sets the reauthentication time for all CSCF subscribers in the *scscf1* S-CSCF service to *500* seconds:

```
update cscf subscriber all cscf-service scscf1 reauthentication-time 500
```

update firewall policy

This command is obsolete.

update ip

When you update an IP Access list, this command forces the new version of the access list to be applied to any subscriber sessions that are currently using that list.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

update ip access-list *list_name* **subscribers [** *command_keyword* **] [** *filter_keywords* **] [| { grep** *grep_options* **| more }]**

list_name

Specifies the name of an existing IP Access list that you want to apply to the subscriber as an alphanumeric string of 1 through 47 characters.

[*command_keyword* **] [** *filter_keywords* **]**

These are the same command keywords and filter keywords available for the **show subscribers** command.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output section* of the *Command Line Interface Overview* chapter in this guide.

Usage

Use this command to force existing subscriber sessions that are already using a specific IP Access list to have that IP Access list reapplied. This is useful when you edit an IP Access list and want to make sure that even existing subscriber sessions have the new changes applied.

Example

To apply the IP Access list named *ACLlist1* to all existing subscribers that are already using that IP Access list, enter the following command:

```
update ip access-list ACLlist1 subscribers all
```

update qos policy map

Updates QoS profile information based on specific subscriber policy maps.

Product

All

Privilege

Security Administrator, Administrator

Syntax

update qos policy-map *map_name* **use-granted-profile-id** *id1* **[** *id2* **] [** *id3* **] subscribers [** *command_keyword* **] [** *filter_keywords* **] [-noconfirm] [verbose] [match-requested-profile-id] [| { grep** *grep_options* **| more }]**

map_name

Specifies the name of an existing policy map as an alphanumeric string of 1 through 15 characters.

use-granted-profile-id *id1* **[** *id2* **] [** *id3* **]**

Specifies the profile IDs to update. Up to three different profile IDs can be specified.
Each profile ID is specified as a hexadecimal value from 0x0 and 0xFFFF.

subscribers [*command_keyword* **] [** *filter_keywords* **]**

These are the same command keywords and filter keywords available for the **show subscribers** command.

[-noconfirm]

Updates matching subscribers without prompting for confirmation.

[verbose]

Displays details for the profile updates.

[match-requested-profile-id]

Sends session-updates only to profile-ids matching the profile-ids in the requested list.

grep *grep_options* **| more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in this guide.

Usage

Use this command to update subscriber session profile IDs based on the specified criteria.

Example

The following command updates profile IDs *0x3E* and *0x4C* for all subscriber sessions and sends session-updates with the IDs:

```
update qos policy-map test use-granted-profile-id 0x3E 0x4C subscribers
all match-requested-profile-id
```

update qos tft

Updates the subscriber traffic flow template (TFT) associated with the flow ID and direction.

Product

All

Privilege

Security Administrator, Administrator

Syntax

update qos tft flow-id *flow-id* **flow-dir { forward | reverse } use-granted-profile-id** *id1* **[** *id2* **] [** *id3* **] subscribers [** *command_keyword* **] [** *filter_keywords* **] [-noconfirm] [verbose] [match-requested-profile-id] [| { grep** *grep_options* **| more }**

flow-id *flow-id*

Sends session updates only when the flow ID matches the flow-id and flow-direction. *flow-id* must be specified as an integer from 1 through 255.

flow-dir { forward | reverse }

Specifies the direction of the TFT flow.

subscribers [*command_keyword* **] [** *filter_keywords* **]]**

These are the same command keywords and filter keywords available for the **show subscribers** command.

Usage

Supports QoS updates based on subscriber TFTs.

Example

```
update qos tft flow-id 0 flow-dir reverse use-granted-profile-id 0x0
subscribers all -noconfirm
```

upgrade

Installs major software releases to the system.

Product

All

Privilege

Security Administrator, Administrator

Syntax

upgrade { online | patch } *image_url* **config** *cfg_url* **[-noconfirm]**

online

Perform a software upgrade from one release version to another. The online upgrade is only available for software release 3.5 and higher.

patch

Install an interim, or patch, software release.

Important: Software Patch Upgrades are not supported in this release.

image_url

Specifies the location of a image file to use for system startup. The URL may refer to a local or a remote file. The URL must be formatted as follows:
[**file:**]{ **/flash** | **/pcmcia1** | **/hd** }[**/***directory*]**/***file_name*
[http: | tftp:]//{ *host*[*:port#*] }[**/***directory*]**/***file_name*

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.
filename is the actual file of interest.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

Important: A file intended for use on an ASR 5000 uses the convention xxxxx.ASR5000.bin, where xxxxx is the software build information.

Important: When using the TFTP, you should use a server that supports large blocks, per RFC 2348. This can be implemented by using the "block size option" to ensure that the TFTP service does not restrict the file size of the transfer to 32MB.

config *config_path*

Specifies the location of a configuration file to use for system startup. This must be formatted as follows:

[**file:**]{ **/flash** | **/pcmcia1** | **/hd** }[**/***path*]**/***filename*
Where *path* is the directory structure to the file of interest, and *filename* is the name of the configuration file. This file typically has a **.cfg** extension.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use the **upgrade online** command to perform a software upgrade when upgrading from one software release version to another, providing that both versions support this feature. For example, you can use this method to upgrade from release version 3.5 (any build number) to version 4.0 (any build number), but you cannot use this method to upgrade from release version 3.0 to version 3.5 since version 3.0 does not support the feature.

Important: Software Patch Upgrades are not supported in this release.

Important: This command is not supported on all platforms.

Example

The following command performs a major software release upgrade from an older version to a newer version. In this example the new software image file is in a subdirectory on a tftp server, and the configuration file is in a subdirectory on the local flash at tftp://host[/path]/filename.

```
upgrade online tftp://imageserver/images/image.bin config
/flash/configurations/localconfig.cfg
```

upgrade content-filtering

Upgrades the Static Rating Database (SRDB) for Category-based Content Filtering application.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

```
upgrade content-filtering category { database | rater-pkg }
```

upgrade content-filtering category database

Triggers the upgrade of the Category-based Content Filtering Static Rating Database (SRDB).

upgrade content-filtering category rater-pkg

Triggers manual upgrade of the Dynamic Content-Filtering Rater Package (**rater.pkg** file).
The **rater.pkg** file contains the models and feature counters that are used to return the dynamic content rating. The upgrade will trigger distribution of the **rater.pkg** to all the SRDBs.

Important: This command is customer specific. For more information, please contact your local sales representative.

Usage

Use this command to load the Static Rating Database (SRDB) in to memory for Category-based Content Filtering application, and/or to load the *rater.pkg* file.
If the default directory of /cf does not exist on the flash, it will create the same. It also locates the recent full database and loads it into memory. This command also clears the old and excess incremental databases.

Important: This command is not supported on all platforms.

Example

The following command upgrades the SRDB for the Category-based Content Filtering application:

```
upgrade content-filtering category database
```

upgrade tethering-detection

Upgrades the Tethering Detection feature's database(s).

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
upgrade tethering-detection database { all | os-signature | tac | ua-signature } [ -
noconfirm ]
```

all

Upgrades all Tethering Detection databases—OS, TAC and UA.

os-signature

Upgrades only the OS database.

tac

Upgrades only the TAC database.

ua-signature

Upgrades only the UA database.

- noconfirm

Executes the command without any prompts and confirmation from the user.

Usage

Use this command to upgrade the database(s) used by the Tethering Detection feature.
This command upgrades the database(s) from file(s) kept in designated path. The name of the existing source file is prefixed with the word "new-". For example for OS DB, if the existing file name is "os-db", the upgrade file name is "new-os-db".
If there is a file named "new-xxx-db", it is verified that it is a valid Tethering Detection database and then loaded it into memory. If successful, the files is renamed "xxx-db" to "xxx-db-<number>" and then renamed "new-xxx-db" to "new-xxx-db".
For example, the command **upgrade tethering-database ua-signature -noconfirm** results in loading the file by name "new-ua-db" if it is present in the designated directory. In case of a successful upgrade, the previous version of the database is stored as backup in a file named "ua-db-1". Also, the newly uploaded database file is renamed as "ua-db".
Also see the **tethering-database** command in the *ACS Configuration Mode Commands* chapter.

Example

The following command upgrades all Tethering Detection databases:

```
upgrade tethering-detection database all -noconfirm
```

upgrade url-blacklisting database

Upgrades the URL blacklisting database.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

```
upgrade url-blacklisting database [ -noconfirm ]
```

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to upgrade and load a URL blacklisting database whenever required.

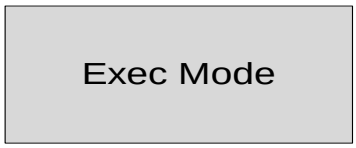
Example

```
upgrade url-blacklisting database
```

Chapter 114
Exec Mode Show Commands (A-C)

This section includes the commands **`show aaa`** through **`show css service`**.

The Exec Mode is the initial entry point into the command line interface system. Exec mode **show** commands are useful in troubleshooting and basic system monitoring.



show aaa

Displays AAA (Authentication Authorization and Accounting) statistics for the current context.

Product

PDSN, GGSN, SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show aaa { group { all | name *aaa_group_name* **} | local counters } [| { grep** *grep_options* **| more }]**

group { all | name *aaa_group_name* **}**

Displays AAA information.

- **all**: If the exec context is local, information for all the default AAA groups, and the AAA groups configured in all the contexts are displayed. If the exec context is not local, information for only the context-specific AAA groups are displayed.
- **name** *aaa_group_name*: Displays information for an existing AAA group specified as an alphanumeric string of 0 through 64 characters.

local counters

Displays information for current context.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command.You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

This command is used to view accounting and authentication statistics for the current context.

Example

The following command displays AAA statistics for the current context:

```
show aaa local counters
```

The following command displays AAA statistics for the AAA group *aaa_group1*:

```
show aaa group name aaa_group1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging analyzer statistics

Displays statistical information for protocol analyzers.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging analyzer statistics [name *protocol* **[verbose]] [| { grep** *grep_options* **| more }]**

---

name *protocol*

Displays detailed information for the specified protocol analyzer:

- **dns**
- **file-transfer**
- **ftp**
- **http**
- **icmp**
- **icmpv6**
- **imap**
- **ip**
- **ipv6**
- **mms**
- **p2p**
- **pop3**
- **pptp**
- **rtcp**
- **rtp**
- **rtsp**
- **sdp**
- **secure-http**
- **sip**
- **smtp**
- **tcp**
- **tftp**
- **udp**
- **wsp**
- **wtp**

verbose

Displays as much information as possible. If this option is not specified then the output is the standard level which is the concise mode.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command.You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display statistic information for active charging protocol analyzers.

Example

The following command displays detailed statistic information for all P2P protocol analyzers:

```
show active-charging analyzer statistics name p2p verbose
```

The following command displays detailed statistic information for all TCP protocol analyzers:

```
show active-charging analyzer statistics name tcp verbose
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging bandwidth-policy

Displays information on bandwidth policies configured in a service.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging bandwidth-policy { all | name *bandwidth_policy_name* **} [| { grep** *grep_options* **| more }]**

all

Displays information for all bandwidth policies configured in the service.

name *bandwidth_policy_name*

Displays detailed information for an existing bandwidth policy specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command.You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view information on bandwidth policies configured in a service.

Example

The following command displays detailed information for the bandwidth policy named *standard*:

```
show active-charging bandwidth-policy nam standard
```

show active-charging charging-action

Displays information for charging actions configured in the Active Charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging charging-action { { { all | name charging_action_name } [ service
name acs_service_name ] } | statistics [ name charging_action_name ] } [ | { grep
grep_options | more } ]
```

all

Displays information for each configured charging action.

name *charging_action_name*

Displays detailed information for an existing charging action specified as an alphanumeric string of 1 through 63 characters.

statistics

Displays statistical information for all configured charging actions.

service name *acs_service_name*

Displays information for all or a specific charging action in the specified ACS. *acs_service_name* is an alphanumeric string of 1 through 15 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command.You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information for charging actions configured in a service.

Example

The following command displays a detailed information for all charging actions:

```
show active-charging charging-action all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging content-filtering category policy-id

Displays Content Filtering (CF) category policy definitions. This command is not available on StarOS 8.0 and earlier releases.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging content-filtering category policy-id { all | id *policy_id* **} [| { grep** *grep_options* **| more }]**

all

Displays definitions of all Content Filtering category policies.

id *policy_id*

Displays definitions of an existing Content Filtering category policy specified as an integer from 1 through 4294967295.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view Content Filtering category definitions for a specific/all Policy IDs.

Example

The following command displays Content Filtering category definitions for policy ID *3*:

```
show active-charging content-filtering category policy-id id 3
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging content-filtering category statistics

Displays category-based content filtering statistics.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging content-filtering category statistics [rulebase { name *rulebase_name* **| all }] [verbose] [| { grep** *grep_options* **| more }]**

rulebase { name *rulebase_name* **| all }**

Displays category-based content filtering statistics, either for all or for a specific rulebase.

- **name** *rulebase_name*: Specifies an existing rulebase as an alphanumeric string of 1 through 63 characters.
- **all**: Displays category-based content filtering statistics for each rulebase in the ACS.

verbose

Displays as much information as possible. If this option is not specified then the output is the standard level, which is the concise mode.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view category-based content filtering statistics for a specific rulebase, or cumulative statistics for all rulebases in the ACS.

Example

The following command displays category-based content filtering statistics for the rulebase named *consumer*:

```
show active-charging content-filtering category statistics rulebase name
consumer
```

The following command displays cumulative category-based content filtering statistics for all rulebases in verbose mode:

```
show active-charging content-filtering category statistics verbose
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging content-filtering server-group

Displays information for Content Filtering Server Group (CFSG) configured in the service.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging content-filtering server-group [name *cfsg_name* **| statistics [name** *cfsg_name* **[acsmgr instance** *instance* **[priority** *priority* **]] | verbose**] [**| { grep** *grep_options* **| more }]**

name *cfsg_name*

Specifies name of an existing CFSG as an alphanumeric string of 1 through 63 characters.

acsmgr instance*instance*

Specifies the manager instance as an integer from 1 through 65535.

priority *priority*

Specifies the priority of the server for which statistics has to be displayed as an integer from 1 through 65535.

verbose

Displays all available statistics of each Internet Content Adaptation Protocol (ICAP) server connection at each instance. If this option is not specified then the output is at the standard level, which is the concise mode.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view CFSG information/statistics.
show active-charging content-filtering server-group name *cfsg_name*: The output of this command displays detailed information for the specified CFSG.
show active-charging content-filtering server-group statistics name *cfsg_name*: The output of this command displays cumulative statistics for the specified CFSG. This will include all the instances and all the servers configured in the CFSG.
show active-charging content-filtering server-group statistics name *cfsg_name* **acsmgr instance** *instance*: The output of this command displays the cumulative statistics of all the ICAP server connections on the specified manager instance.

show active-charging content-filtering server-group statistics name *cfsg_name* **acsmgr instance** *instance* **priority** *priority*: The output of this command displays the statistics for the specified ICAP server connection on the specified manager instance.
show active-charging content-filtering server-group statistics verbose: The output of this command displays statistics of each ICAP server connection at each instance.

Example

The following command displays information for the CFSG named *test12*:

```
show active-charging content-filtering server-group name test12
```

The following command displays detailed information for all CFSGs:

```
show active-charging content-filtering server-group statistics verbose
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging credit-control

D displays statistics for Diameter/RADIUS Prepaid Credit Control Service in the Active Charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging credit-control { statistics [all | group *group_name* **] | session-states [rulebase** *rulebase_name* **] [content-id** *content_id* **] } [| { grep** *grep_options* **| more }]**

---

statistics [all | group *group_name* **]**

Displays prepaid credit control statistics.

- **all**: Displays all available statistics.
- **group** *group_name*: Displays statistics for an existing credit control group specified as an alphanumeric string of 1 through 63 characters.

---

session-states [rulebase *rulebase_name* **] [content-id** *content_id* **]**

Displays prepaid CCA session status based on rulebase and/or content ID.

- **rulebase** *rulebase_name*: Displays the Credit Control Application (CCA) session state counts for an existing rulebase specified as an alphanumeric string of 1 through 63 characters.
- **content-id** *content_id*: Displays CCA session state counts for a content ID of a credit control service specified as an integer from 1 through 65535.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view statistics for Diameter/RADIUS prepaid credit control service in the ACS.

Example

The following command shows ACS statistics of configured Diameter or RADIUS Credit Control Application:

```
show active-charging credit-control statistics
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging dns-learnt-ip-addresses

Displays DNS learnt IP address statistics for the DNS Snooping feature.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging dns-learnt-ip-addresses statistics { sessmgr { all | instance *sessmgr_instance* **} [verbose] | summary } [| { grep** *grep_options* **| more }]**

---

sessmgr { all | instance *sessmgr_instance* **} [verbose]**

Displays information for all or the specified Session Manager (SessMgr) instance.

- **all**: Displays information for all SessMgr instances.
- **instance** *sessmgr_instance*: Displays information for a SessMgr instance specified as an integer from 1 through 65535.
- **verbose**: Displays detailed statistics for specified criteria. Use this keyword to view the learnt IP addresses.

---

summary

Displays summary information.

| { grep *grep_options* **| more }**

Specifies that the output of this command is to be piped (sent) to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view statistics for the DNS Snooping feature related DNS learnt-ip-addresses.
This command displays the number of learnt IP entries per rule line. It displays on a service level the number of resolved (learnt) IP addresses per rule line per rulebase (once if a rule line is used multiple times in the same rulebase as it is shared across rulebase) per destination context per SessMgr instance. It also displays the number of entries flushed due to TTL expiry. The field entries_replaced gives the number of entries replaced (same IP returned again) in the pool due to a DNS response by same/another subscriber for same domain-name, wherein the TTL of the entry will be replaced.
IPv4-overflows will start incrementing when the maximum limit of 51200 across system is reached OR limit of 200 per pattern is reached.
Ipv6-overflows will start incrementing when maximum limit of 25600 across system is reached OR limit of 100 per pattern is reached.
Limits are:

- Maximum of 51,200 IPv4 entries per instance shared across IPv4 all pools.
- Maximum of 200 IPv4 entries per pool (pool is same as discussed before (per rule-line pattern)).
- Maximum of 25,600 IPv6 entries per instance shared across all IPv6 pools.

- Maximum of 100 IPv6 entries per pool.

Example

The following command displays summary statistics for DNS learnt IP addresses:

```
show active-charging dns-learnt-ip-addresses statistics summary
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging edr-format

Displays information about Event Data Record (EDR) formats configured in the Active Charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging edr-format [statistics] [all | name *edr_format_name* **] [| { grep** *grep_options* **| more }]**

all

Displays information for all EDR formats.

statistics

Displays statistics for all or an existing EDR format.
If neither **all** nor **name** is specified, summarized statistics over all EDR formats is displayed.

name *edr_format_name*

Displays information for an existing EDR format specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information for EDR format(s) in the ACS.

Example

The following command displays all configured EDR formats in the ACS.

```
show active-charging edr-format all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging edr-udr-file

Displays CDR flow control information. This command also displays the Event Data Record (EDR) and Usage Data Record (UDR) file information.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging edr-udr-file { flow-control-counters [ verbose ] | statistics } [ |
{ grep grep_options | more } ]
```

flow-control-counters [verbose]

Displays the counters for dropped EDR/UDR records. These counters are for when CDRMOD uses flow control to stop ACS/Session Managers from sending the records.
verbose displays detailed information.

statistics

Displays EDR and UDR file statistics.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command.You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view CDR flow control information.

Example

The following command displays EDR and UDR files statistics:

```
show active-charging edr-udr-file statistics
```

The following command displays CDR flow control information:

```
show active-charging edr-udr-file flow-control-counters
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging file-space-usage

Displays the file space used by Charging Data Record (CDR) and Event Data Record (EDR) files.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging file-space-usage [| { grep *grep_options* **| more }]**

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view CDR/EDR file space usage information. The context in which this command is used is not relevant.

show active-charging firewall statistics

Displays Active Charging Stateful Firewall statistics.

Product

FW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging firewall statistics [callid *call_id* **| domain-name** *domain_name* **| nat-realm** *nat_realm* **| protocol { icmp | icmpv6 | ip | ipv6 | other | tcp | udp } | username** *user_name* **] [acsmgr instance** *instance_id* **] [verbose] [| { grep** *grep_options* **| more }]**

acsmgr instance *instance_id*

Specifies the ACS/Session Manager instance ID as an integer from 1 through 65535.

callid *call_id*

Specifies the call identification number as an 8-digit hexadecimal number.

domain-name *domain_name*

Specifies the domain name as an alphanumeric string of 1 through 127 characters.

nat-realm *nat_realm*

Specifies the NAT realm name as an alphanumeric string of 1 through 31 characters.

protocol { icmp | ip | other | tcp | udp }

Specifies the protocol:

- **icmp**: ICMPv4
- **icmpv6**
- **ip**: IPv4
- **ipv6**
- **other**: Protocols other than TCP, UDP, and ICMPv4/ICMPv6.
- **tcp**
- **udp**

username *user_name*

Specifies the user name as an alphanumeric string of 1 through 127 characters.

verbose

Displays all available information. If this option is not specified then the output is the standard level, which is the concise mode.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view Stateful Firewall statistics. If you are in the local context, statistics for all contexts are displayed. Otherwise, only statistics of your current context are displayed.

Example

The following command displays Stateful Firewall statistics:

```
show active-charging firewall statistics
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging firewall track-list

Displays the list of servers being tracked for involvement in any Denial-of-Service (DOS) attacks.

Product

FW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging firewall track-list attacking-servers [ | { grep grep_options | more } ]
```

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view details of servers being tracked for involvement in any DOS attack.

Example

The following command displays the list of servers being tracked for involvement in any DOS attacks:

```
show active-charging firewall track-list attacking-servers
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging flows

Displays information for active charging flows.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging flows { all | [connected-time [< | > | greater-than | less-than] *seconds* **] [flow-id** *flow_id* **] [full] [idle-time [< | > | greater-than | less-than]** *seconds* **] [ip-address [server | subscriber] [< | > | IPv4 | greater-than | less-than]** *address* **] [nat { not-required | required [nat-ip** *nat_ip_address* **] }] [pacing-bitrate [< | > | = | greater-than | less-than | equal-to]** *number* **[port-number [server | subscriber] [< | > | IPv4 | greater-than | less-than]** *number* **] [rx-bytes [< | > | greater-than | less-than]** *number* **] [rx-packets [< | > | greater-than | less-than]** *number* **] [session-id** *session_id* **] [summary] [trans-proto { icmp | tcp | udp }] [tx-bytes [< | > | greater-than | less-than]** *number* **] [tx-packets [< | > | greater-than | less-than]** *number* **] [type** *flow_type* **] } [| { grep** *grep_options* **| more }]**

---

all

Displays information for all active charging flows.

---

connected-time [< | > | greater-than | less-than] *seconds*

Displays information for flows filtered by connected time period.

- **<** *seconds*: Displays flows that have been connected less than the specified number of seconds.
- **>** *seconds*: Displays flows that have been connected more than the specified number of seconds.
- **greater-than** *seconds*: Displays flows that have been connected more than the specified number of seconds.
- **less-than** *seconds*: Displays flows that have been connected less than the specified number of seconds.

seconds is an integer from 0 through 4294967295.

---

flow-id *flow_id*

Displays concise information for specified active charging flow ID.

---

full

Displays all available information for the specified flows.

---

idle-time [< | > | greater-than | less-than] *seconds*

Displays information for flows filtered by idle time period.

- **<** *seconds*: Displays flows that have been idle less than the specified number of seconds.
- **>** *seconds*: Displays flows that have been idle more than the specified number of seconds.

- **greater-than** *seconds*: Displays flows that have been idle more than the specified number of seconds.
- **less-than** *seconds*: Displays flows that have been idle less than the specified number of seconds.

seconds is an integer from 0 through 4294967295.

---

ip-address [server | subscriber] [< | > | IPv4 | greater-than | less-than] *address*

Displays information for flows filtered by IPv4 IP address.

- **server**: Specifies the IP address for a specific server.
- **subscriber**: Displays subscriber details for the IP address specified in IPv4 dotted-decimal format.
- **<** *address*: Specifies an IPv4 IP address that is less than *address*.
- **>** *address*: Specifies an IPv4 IP address that is greater than *address*.
- **greater-than** *address*: Specifies an IPv4 IP address that is greater than *address*.
- **less-than** *address*: Specifies an IPv4 IP address that is less than *address*.

address is an IP address expressed in IPV4 dotted-decimal notation.

---

nat { not-required | required [nat-ip *nat_ip_address* **[nat-port** *nat_port* **]] }**

Important: The **nat** keyword and options are only available in StarOS 8.3 and later releases.

Displays information for flows filtered by Network Address Translation (NAT) required or not required setting.

- **not-required**: Sessions with NAT processing are not required.
- **required**: Sessions with NAT processing are required.
- **nat-ip** *nat_ip_address*: Sessions using the NAT IP address expressed in IPv4 dotted-decimal notation.
- **nat-port** *nat_port*: Sessions using the specified NAT IP address and NAT port number specified as an integer from 0 through 65535.

---

pacing-bitrate [< | > | = | greater-than | less-than | equal-to] *number*

Displays information on video flows filtered by a video pacing bit rate specified an integer from 1 to 256000000.

- **<** *number*: Specifies a number that is less than the specified video pacing bit rate.
- **>** *number*: Specifies a number that is greater than the specified video pacing bit rate.
- **=** *number*: Specifies a number that is equal to the specified video pacing bit rate.
- **greater-than** *number*: Specifies a number that is greater than the specified video pacing bit rate.
- **less-than** *number*: Specifies a number that is less than the specified video pacing bit rate
- **equal-to** *number*: Specifies a number that is equal to the specified video pacing bit rate.

---

port-number [server | subscriber] [< | > | IPv4 | greater-than | less-than] *_number*

Displays information on flows filtered by port number.

- **server**: Specifies the port-number for a specific server.

- **subscriber**: Specifies subscriber details for this port-number expressed as an integer from 0 through 65535.
- **<** *number*: Specifies a port number that is less than the specified port-number.
- **>** *number*: Specifies a port number that is greater than the specified port-number.
- **greater-than** *number*: Specifies a port number that is greater than the specified port-number.
- **less-than** *number*: Specifies a port number that is less than the specified port-number.

---

rx-bytes [< | > | greater-than | less-than] *number*

Displays information on flows filtered by the number of bytes received in the flow.

- **<** *number*: Specifies the number of bytes that is less than the specified rx-bytes.
- **>** *number*: Specifies number of bytes that is greater than the specified rx-bytes.
- **greater-than** *number*: Specifies number of bytes that is greater than the specified rx-bytes.
- **less-than** *number*: Specifies number of bytes that is less than the specified rx-bytes.

number must be an integer from 0 through 18446744073709551615.

---

rx-packets [< | > | greater-than | less-than] *number*

Displays information on flows filtered by the number of packets received in the flow.

- **greater-than** *number*: Specifies the number of packets that is greater than the specified rx-packets.
- **less-than** *number*: Specifies the number of packets that is less than the specified rx-packets.

number must be an integer from 0 through 18446744073709551615.

---

session-id *session_id*

Displays detailed information for specific active charging session ID.

---

summary

Displays summary information for defined sessions, based on defined parameters.

---

trans-proto { icmp | tcp | udp }

Displays information on flows filtered by the transport protocol.

- **icmp**: ICMP protocol type flow
- **tcp**: TCP protocol type flow
- **udp**: User Datagram Protocol (UDP) flows

---

tx-bytes [< | > | greater-than | less-than] *number*

Displays information on flows filtered by the number of bytes received in the flow.

- **<** *number*: Specifies the number of bytes that is less than the specified tx-bytes.
- **>** *number*: Specifies number of bytes that is greater than the specified tx-bytes.
- **greater-than** *number*: Specifies number of bytes that is greater than the specified tx-bytes.
- **less-than** *number*: Specifies number of bytes that is less than the specified tx-bytes.

number must be an integer from 0 through 18446744073709551615.

tx-packets [< | > | greater-than | less-than] *number*

Displays information on flows filtered by the number of packets received in the flow.

- **greater-than** *number*: Specifies the number of packets that is greater than the specified tx-packets.
- **less-than** *number*: Specifies the number of packets that is less than the specified tx-packets.

number must be an integer from 0 through 18446744073709551615.

type *flow_type*

Displays information on flows filtered by flow type of application protocol.
flow_type must be one of the following:

- **dns**
- **ftp**
- **http**
- **icmp**
- **icmpv6**
- **imap**
- **ip**
- **ipv6**
- **mms**
- **p2p**: P2P protocol type flows including one or more of the following applications:
  - **actsync**
  - **aimini**
  - **antsp2p**
  - **applejuice**
  - **ares**
  - **armagettron**
  - **battlefd**
  - **bittorrent**
  - **blackberry**
  - **citrix**
  - **clubpenguin**
  - **crossfire**
  - **ddlink**
  - **directconnect**
  - **dofus**
  - **edonkey**
  - **facebook**
  - **facetime**

Important: The **facetime** protocol is available only in releases 9.0 and 11.0. This protocol is not available in release 10.0.

- **fasttrack**
- **feidian**
- **fiesta**
- **filetopia**
- **florensia**
- **freenet**
- **fring**
- **funshion**
- **gadu_gadu**
- **gamekit**

Important: The **gamekit** protocol is available only in releases 9.0 and 11.0. This protocol is not available in release 10.0.

- **gmail**
- **gnutella**
- **gtalk**
- **guildwars**
- **halflife2**
- **hamachivpn**
- **iax**
- **icecast**
- **imesh**
- **imo**
- **iptv**
- **irc**
- **isakmp**
- **iskoot**
- **itunes**
- **jabber**
- **kontiki**
- **manolito**
- **maplestory**
- **meebo**
- **mgcp**

- msn
- mute
- mypeople
- myspace
- netmotion
- nimbuzz
- octoshape
- off
- ogg
- oovoo
- openft
- openvpn
- orb
- oscar
- paltalk
- pando
- pandora
- popo
- pplive
- ppstream
- ps3
- qq
- qqgame
- qqlive
- quake
- quicktime
- rdp
- rdt
- rfactor
- rmstream
- scydo
- secondlife
- shoutcast
- skinny
- skype
- slingbox
- sopcast

- soulseek
- splashfighter
- spotify
- ssdp
- stealthnet
- steam
- stun
- tango
- teamspeak
- teamviewer
- thunder
- tor
- truphone
- tunnelvoice
- tvants
- tvuplayer
- twitter
- ultrabac
- usenet
- uusee
- veohtv
- viber
- vpnx
- vtun
- warcft3
- whatsapp
- wii
- winmx
- winny
- wmstream
- wofkungfu
- wofwarcraft
- xbox
- xdcc
- yahoo
- yourfreetunnel
- zattoo

- **pop3**
- **pptp**
- **rtcp**
- **rtp**
- **rtsp**
- **secure-http**
- **sip**
- **smtp**
- **tcp**
- **tftp**
- **udp**
- **unknown**: Unknown type of protocol type flow not listed here.
- **wsp-connection-less**
- **wsp-connection-oriented**

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display charging flow type information.

Example

The following command displays a detailed flow information for a session ID of *test*:

```
show active-charging flows session-id test
```

The following command displays a detailed flow information for a P2P type session:

```
show active-charging flows full type p2p
```

The following command displays a detailed information for a P2P type flow:

```
show active-charging flows type p2p
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging flow-mappings

Displays information about all the active flow mappings based on the applied filters.

Product

FW, NAT

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging flow-mappings [all | call-id *callid* **| [nat { not-required | required [nat-realm** *realm_name* **] } | trans-proto { tcp | udp }] + [| { grep** *grep_options* **| more }]**

all

Displays the all the available active charging flow-mapping information.

call-id *callid*

Displays detailed information for a call ID specified as an 8-digit hexadecimal number.

nat { required [nat-realm *string* **] not-required }**

Displays the active charging flow mappings for which NAT is enabled or disabled.

trans-proto { tcp | udp }

Displays the transport layer.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view the Active Charging flow-mapping details.

Example

The following command displays the total number of Active Charging flow-mappings:

```
show active-charging flow-mappings all
```

The following command displays the flow-mappings for which NAT is enabled and the NAT-realm used is *natpool3*:

```
show active-charging flow-mappings nat required nat-realm natpool3
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging fw-and-nat policy

Displays Firewall-and-NAT Policy information.

Important: This command is only available in StarOS 8.1, and in StarOS 9.0 and later. For more information on this command please contact your local service representative.

Product

ACS, FW, NAT

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging fw-and-nat policy { { { all | name *fw_nat_policy_name* **} [service name** *acs_service_name* **] } | { statistics { all | name** *fw_nat_policy_name* **} } } [| { grep** *grep_options* **| more }]**

all

Displays information for all Firewall-and-NAT policies configured, optionally all in a specified service.

name *fw_nat_policy_name*

Displays detailed information for an existing Firewall-and-NAT policy specified as an alphanumeric string of 1 through 63 characters.

service name *acs_service_name*

Displays information for all or the specified Firewall-and-NAT policy in the specified ACS.
acs_service_name must be the name of the ACS expressed as an alphanumeric string of 1 through 15 characters.

statistics

Displays statistics for all or the specified Firewall-and-NAT policy.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view Firewall-and-NAT Policy information.

Example

The following command displays detailed information for the Firewall-and-NAT policy named *standard*:

```
show active-charging fw-and-nat policy name standard
```

show active-charging group-of-prefixed-urls

D displays information on group of prefixed URLs configured in an Active Charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging group-of-prefixed-urls { all | name *prefixed_url_group* **} [service name** *acs_service_name* **] [| { grep** *grep_options* **| more }]**

all

Displays information for all group of prefixed URLs configured in an ACS.

name *prefixed_url_group*

Displays detailed information for the group of prefixed URLs specified as an alphanumeric string of 1 through 63 characters.

service name *acs_service_name*

Displays information for all or the specified group of prefixed URLs in the specified ACS. *acs_service_name* must be the name of the ACS expressed as alphanumeric string of 1 through 15 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter

Usage

Use this command to view information on group of prefixed URLs configured in the ACS.

Example

The following command displays for the group of prefixed URLs named *test123*:

```
show active-charging group-of-prefixed-urls name test123
```

show active-charging group-of-ruledefs

Displays information for all groups or a specified group of ruledefs configured in the Active Charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging group-of-ruledefs { { all | name *group_of_ruledefs* **} [service name** *acs_service_name* **] | statistics name** *group_of_ruledefs* **} [| { grep** *grep_options* **| more }]**

all

Displays information for all groups of ruledefs configured, optionally all in a specified ACS.

name *group_of_ruledefs*

Displays detailed information for an existing group of ruledefs specified as an alphanumeric string of 1 through 63 characters.

service name *acs_service_name*

Displays information for all groups or the specified group of ruledefs within the ACS. *acs_service_name* must be the name of the ACS expressed as an alphanumeric string of 1 through 15 characters.

statistics name *group_of_ruledefs*

Displays statistics for an existing group of ruledefs specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view information on group of ruledefs configured in a ACS.

Example

The following command displays information on all groups of ruledefs configured:

```
show active-charging group-of-ruledefs all
```

show active-charging nat statistics

Displays Network Address Translation (NAT) realm statistics.

Product

NAT

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging nat statistics [nat-realm *nat_realm* **[summary]] [| { grep** *grep_options* **| more }]**

show active-charging nat statistics

When issued in the local context, this command displays statistics for all NAT realms in all contexts. When issued in a specific context, this command displays statistics for all NAT realms in that context.

show active-charging nat statistics nat-realm *nat_realm*

When issued in the local context, this command displays statistics for the specified NAT realm in all contexts. When issued in a specific context, this command displays statistics for the specified NAT realm in that context.

nat-realm *nat_realm*

Specifies the NAT realm's / NAT realm group's name as an alphanumeric string of 1 through 31 characters.

summary

When the *nat_realm* specified is a "pool group" and the **summary** option is used, summary statistics of all pools in the pool group are displayed.
When the *nat_realm* specified is a pool and the **summary** option is not used, all available statistics for the specified pool are displayed.
When the *nat_realm* specified is a "pool group" and the **summary** option is not used, all available statistics of each pool in the specified "pool group" are displayed.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view NAT realm statistics.

Example

The following command when issued in the local context, displays NAT realm statistics for NAT realms named *test135* in all contexts:

```
show active-charging nat statistics nat-realm test135
```

show active-charging packet-filter

D displays information on packet filters configured in an Active Charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging packet-filter { all | name *packet_filter_name* **} [service name** *acs_service_name* **] [| { grep** *grep_options* **| more }]**

all

Displays information for all packet filters configured, optionally all configured in an ACS.

name *packet_filter_name*

Displays detailed information for an existing packet filter specified as an alphanumeric string of 1 through 63 characters.

service name *acs_service_name*

Displays information for all filters or the specified packet filter in the specified ACS. *acs_service_name* must be the name of the ACS expressed as an alphanumeric string of 1 through 15 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view information on packet filters configured in an ACS.

Example

The following command displays information for the packet filter *filter12*:

```
show active-charging packet-filter name filter12
```

show active-charging rulebase

Displays information for ACS rulebases.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging rulebase { { { all | name rulebase_name } [ service name
acs_service_name ] } | statistics [ name rulebase_name ] } | [ | { grep grep_options |
more } ]
```

all

Displays details of all rulebases configured in the system.

name *rulebase_name*

Displays details of an existing rulebase specified as an alphanumeric string of 1 through 63 characters.

service name *acs_service_name*

Displays details of all or the specified rulebase configured in the specified ACS. *acs_service_name* must be the name of the ACS expressed as an alphanumeric string of 1 through 15 characters.

statistics

Displays statistical information for all or the specified rulebase.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view various statistics for a specific charging rulebase.

Example

The following command displays active charging rulebase statistics.

```
show active-charging rulebase statistics
```

The following command displays configurations and statistics for a rulebase named *rulebase_1*.

```
show active-charging rulebase name rulebase_1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging ruledef

Displays information for rule definitions (ruledefs) configured in the Active Charging Service (ACS).

Product

ACS, FW, TPO

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging ruledef { all | charging | firewall | name *ruledef_name* **| post-processing | routing | statistics [all { charging | firewall [wide] | post-processing | tpo } | name** *ruledef_name* **[wide]] | tpo } [| { grep** *grep_options* **| more }]**

all

Displays information for all ruledefs configured in the ACS.

charging

Displays information for all Charging ruledefs configured in the ACS.

firewall

Displays information for all Stateful Firewall ruledefs configured in the ACS.

name *ruledef_name*

Displays detailed information for an existing ruledef specified as an alphanumeric string of 1 through 63 characters.

post-processing

Important: This keyword is only available in StarOS 8.3 and later.

Displays information for all post-processing ruledefs configured in the ACS.

routing

Displays information for all Routing ruledefs configured in the ACS.

service *service_name*

This keyword is obsolete.

statistics [all { charging | firewall [wide] | post-processing | tpo } | name *ruledef_name* **[wide]]**

Displays statistical information for all/specified ruledefs configured in the ACS. If none of the optional arguments are supplied, statistics totaled for all ruledefs will be displayed.

- **all**: Displays statistics for all ruledefs of the specified type configured in the ACS.
- **charging**: Displays statistics for all Charging ruledefs configured in the ACS.

- **firewall**: Displays statistics for all Firewall ruledefs configured in the service.
- **post-processing**: Displays statistics for all Post-processing ruledefs configured in the ACS.

> **Important:** The **post-processing** keyword is available only in StarOS 8.3 and later releases.

- **tpo**: Displays statistics for all Traffic Performance Optimization (TPO) ruledefs configured in the ACS.

> **Important:** The **tpo** keyword is available only in 12.2 and later releases.

- **name** *ruledef_name*: Displays statistics for an existing ruledef specified as an alphanumeric string of 1 through 63 characters.
- **wide**: Displays all available information in a single wide line.

tpo

> **Important:** The **tpo** keyword is available only in 12.2 and later releases.

Displays information for all Traffic Performance Optimization (TPO) ruledefs configured in the ACS.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view information for ruledefs configured in the ACS.

Example

The following command displays ACS ruledef statistics.

```
show active-charging ruledef statistics
```

> **Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging service

Displays detailed information about an Active Charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging service { all | name acs_service_name } [ | { grep grep_options |
more } ]
```

all

Displays information for all configured ACSs.

name *acs_service_name*

Displays detailed information for the ACS specified as an alphanumeric string of 1 through 15 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view ACS details.

Example

The following command displays details for the ACS named *test1*.

```
show active-charging service name test1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging sessions

Displays statistics for Active Charging Service (ACS) sessions.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging sessions [ full [ wide ] | summary | display-dynamic-charging-rules
| dynamic-charging ] { [ all ] | [ filter_keyword ] + } [ | { grep grep_options | more }
]
```

full [wide]

Displays all available information for the specified session.
Optionally all available information can be displayed in a single wide line.

summary

Displays summary information for defined sessions based on defined parameters.

display-dynamic-charging-rules

Displays information for the dynamic charging rules configured per session under Gx interface support.

dynamic-charging

Displays information for dynamic charging sessions.

filter_keyword

The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all command keywords. Multiple filter keywords can be entered on a command line.
When multiple filter keywords are specified, the output conforms to all of the filter keywords specifications. For example, if you enter the following command:
show active-charging sessions full active-charging-service acs_!
Counters for active charging sessions active in ACS *acs_1* with full details is displayed. Information for all other services is not displayed.

acsmgr instance *instance*

Displays session information for a specific ACS/Session Manager instance.

active-charging-service *acs_service_name*

Displays session information for the ACS specified as an alphanumeric string of 1 through 15 characters.

all

Displays session information for all active charging sessions.

callid

Specifies the call identification number.

display-dynamic-charging-rules

Displays dynamic charging rules configured.

dynamic-charging

Displays session information for all dynamic charging sessions.

firewall { not-required | required }

Displays session information for sessions with Firewall Processing required or not required, as specified.

fw-and-nat policy *fw_nat_policy_name*

Displays information for the Firewall-and-NAT Policy specified as an alphanumeric string of 1 through 63 characters.

imsi

Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session.

ip-address

Specifies the IP address for the specific charging service.

msid

Displays active charging session information for a specific subscriber's Mobile Station Identification (MSID) number.

ipv4

Displays active charging session information with IPv4 Firewall enabled/disabled.

ipv6

Displays active charging session information with IPv6 Firewall enabled/disabled.

nat { not-required | required [nat-realm *nat_realm* **] } [ipv4 | ipv6]**

Displays session information for sessions with NAT required or not required, as specified.
nat-realm *nat_realm* specifies the name of a NAT realm as an alphanumeric string of 1 through 63 characters.
ipv4: Displays active-charging sessions for which NAT44 processing is required.
ipv6: Displays active-charging sessions for which NAT64 processing is required.

rulebase

Displays information for a rulebase that is configured in an active charging session.

rx-data

Displays the bytes received in the session.

session-id

Displays detailed session information for a specific session identification.

tx-data

Displays the bytes sent in the session.

type

Displays session information for specified DNS application type(s).

- **dns**
- **ftp**
- **http**
- **icmp**
- **icmpv6**
- **imap**
- **ip**
- **ipv6**
- **mms**
- **p2p**: Displays session information for a P2P application type:
  - **actsync**
  - **aimini**
  - **antsp2p**
  - **applejuice**
  - **ares**
  - **armagettron**
  - **battlefd**
  - **bittorrent**
  - **blackberry**
  - **citrix**
  - **clubpenguin**
  - **crossfire**
  - **ddlink**
  - **directconnect**
  - **dofus**
  - **edonkey**
  - **facebook**
  - **facetime**

Important: The **facetime** protocol is available only in releases 9.0 and 11.0. This protocol is not available in release 10.0.

- **fasttrack**
- **feidian**
- **fiesta**
- **filetopia**
- **florensia**
- **freenet**
- **fring**
- **funshion**
- **gadu_gadu**
- **gamekit**

Important: The **gamekit** protocol is available only in releases 9.0 and 11.0. This protocol is not available in release 10.0.

- **gmail**
- **gnutella**
- **gtalk**
- **guildwars**
- **halflife2**
- **hamachivpn**
- **iax**
- **icecast**
- **imesh**
- **imo**
- **iptv**
- **irc**
- **isakmp**
- **iskoot**
- **itunes**
- **jabber**
- **kontiki**
- **manolito**
- **maplestory**
- **meebo**
- **mgcp**

- msn
- mute
- mypeople
- myspace
- netmotion
- nimbuzz
- octoshape
- off
- ogg
- oovoo
- openft
- openvpn
- orb
- oscar
- paltalk
- pando
- pandora
- popo
- pplive
- ppstream
- ps3
- qq
- qqgame
- qqlive
- quake
- quicktime
- rdp
- rdt
- rfactor
- rmstream
- scydo
- secondlife
- shoutcast
- skinny
- skype
- slingbox
- sopcast

- soulseek
- splashfighter
- spotify
- ssdp
- stealthnet
- steam
- stun
- tango
- teamspeak
- teamviewer
- thunder
- tor
- truphone
- tunnelvoice
- tvants
- tvuplayer
- twitter
- ultrabac
- usenet
- uusee
- veohtv
- viber
- vpnx
- vtun
- warcft3
- whatsapp
- wii
- winmx
- winny
- wmstream
- wofkungfu
- wofwarcraft
- xbox
- xdcc
- yahoo
- yourfreetunnel
- zattoo

- **pop3**
- **pptp**
- **rtcp**
- **rtp**
- **rtsp**
- **secure-http**
- **sip**
- **smtp**
- **tcp**
- **tftp**
- **udp**
- **unknown**
- **wsp-connection-less**
- **wsp-connection-oriented**

username

Displays session information for a specific user name.

dynamic-charging

Displays the all sessions having received at least one Gx message from Session Manager/IMS Authorization.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display the configuration information for an active charging session.

Example

The following command displays full information of an active charging session.

```
show active-charging sessions full all
```

The following command displays an active charging session summary.

```
show active-charging sessions summary
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging subsystem

Displays service and configuration counters for the ACS.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging subsystem { all | facility acsmgr { all | instance instance_value }
[ rulebase name rulebase_name ] | sip } [ | { grep grep_options | more } ]
```

all

Displays ACS subsystem information.

facility acsmgr [all | instance *instance_value*]

Displays logged events for all ACS/Session Managers or for a specific instance expressed as an integer from 1 through 65535.

rulebase name *rulebase_name*

Displays rulebase statistics for the specified rulebase expressed as an alphanumeric string of 1 through 63 characters.

sip

Displays SIP related statistics.

| { grep *grep_options* | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view ACS/Session Manager information.

Example

The following command displays ACS subsystem information:

```
show active-charging subsystem all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging tcp-proxy statistics

Displays TCP Proxy statistics.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging tcp-proxy statistics [all | ip-layer | proxy-fac | rulebase *rulebase_name* **| socket-migration | tcp-layer] [verbose] [| { grep** *grep_options* **| more }]**

all

Displays all TCP Proxy statistics aggregated over all rulebases, including for both IP and TCP layers.

ip-layer

Displays TCP Proxy statistics for IP layer.

proxy-fac

Displays TCP Proxy Flow Admission Control statistics.

rulebase *rulebase_name*

Displays TCP Proxy statistics for the rulebase specified as an alphanumeric string of 1 through 63 characters.

socket-migration

Displays TCP Proxy statistics for socket migration.

tcp-layer

Displays TCP Proxy statistics for TCP layer.

verbose

Displays detailed TCP Proxy statistics.

| { grep *grep_options* **| more }**

Specifies that the output of this command is to be piped (sent) to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view TCP Proxy statistics.

Example

The following command displays detailed TCP proxy statistics for the rulebase named *test14*:

```
show active-charging tcp-proxy statistics rulebase test14 verbose
```

show active-charging tethering-detection

Displays information/statistics pertaining to Tethering Detection databases.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging tethering-detection { database [ os-signature | tac | ua-signature
]+ [ sessmgr { all | instance instance } ] [ | { grep grep_options | more } ] |
statistics }
```

database [os-signature | tac | ua-signature]+ [sessmgr { all | instance *instance* }]

Displays information pertaining to the specified Tethering Detection database(s).

- **os-signature**: Displays Tethering Detection OS (Operating System) database information.
- **tac**: Displays Tethering Detection TAC (Transaction Authorization Code) database information.
- **ua-signature**: Displays Tethering Detection UA (User Agent) database information.
- **+**: Indicates that more than one of the preceding keywords can be entered in a single command.
- **sessmgr { all | instance** *instance* **}**: Displays SessMgr Tethering Detection database status.
  - **all**: Displays status for all SessMgr instances.
  - **instance** *instance*: Displays status for the SessMgr instance specified as an integer from 1 through 10000.

statistics

Displays Tethering Detection related statistics.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view information/statistics pertaining to Tethering Detection databases.

Example

The following command displays information pertaining to Tethering Detection UA and OS databases:

```
show active-charging tethering-detection database ua-signature os-
signature
```

The following command displays information pertaining to all Tethering Detection databases:

show active-charging tethering-detection database

show active-charging timedef

Displays the details of timeslots configured in specified time definition(s).

Important: This command is only available in StarOS 8.1 and in StarOS 9.0 and later.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging timedef { all | name timedef_name } [ service name acs_service_name
] [ | { grep grep_options | more } ]
```

all

Displays information for all timedefs configured in the service.

name *timedef_name*

Displays detailed information for the timedef specified s an alphanumeric string of 1 through 63 characters.

service name *acs_service_name*

Displays information for all or a specific timedef configured in the specified ACS. *acs_service_name* must be the name of the ACS expressed as an alphanumeric string of 1 through 15 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view details of timeslots configured in specified timedef(s) that have been configured for the Time-of-Day Activation/Deactivation of Rules feature.

Example

The following command displays timeslot details of all timedefs configured in the ACS:

```
show active-charging timedef all
```

show active-charging tpo policy statistics

Displays Traffic Performance Optimization (TPO) policy statistics.

Product

TPO

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging tpo policy statistics [all | name *tpo_policy_name* **] [| { grep** *grep_options* **| more }]**

name *tpo_policy_name*

Displays detailed statistics for an existing TPO policy specified as an alphanumeric string of 1 through 63 characters.

all

Displays statistics for all TPO policies configured in the active charging service.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view TPO policy statistics.

- "**show active-charging tpo policy statistics all**" command displays statistics for each TPO policy configured in the active charging service.
- "**show active-charging tpo policy statistics name** *tpo_policy_name*" command displays statistics for the specified TPO policy.
- "**show active-charging tpo policy statistics**" command displays aggregated statistics for all TPO policies configured in the active charging service.

Example

The following command displays statistics for the TPO policy named *policy12*:

```
show active-charging tpo policy statistics name policy12
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging tpo profile statistics

Displays Traffic Performance Optimization (TPO) profile statistics.

Product

TPO

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging tpo profile statistics [name *tpo_profile_name* **| all] [| { grep** *grep_options* **| more }]**

name *tpo_profile_name*

Displays detailed statistics for an existing TPO profile specified as an alphanumeric string of 1 through 63 characters.

all

Displays statistics for all TPO profiles configured in the active charging service.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view TPO profile statistics.

- "**show active-charging tpo profile statistics all**" command displays statistics for each TPO profile configured in the active charging service.
- **show active-charging tpo profile statistics name** *tpo_profile_name* command displays statistics for the specified TPO profile.
- **show active-charging tpo profile statistics** command displays aggregated statistics for all TPO profiles configured in the active charging service.

Example

The following command displays statistics for the TPO profile named *profile12*:

```
show active-charging tpo profile statistics name porfile12
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging udr-format

Displays information about UDR formats configured in an Active charging Service (ACS).

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging udr-format { all | name udr_fromat_name } [ | { grep grep_options |
more } ]
```

all

Displays information for all UDR formats.

name *udr_fromat_name*

Displays information for an existing UDR format specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information for UDR format(s) in an ACS.

Example

The following command displays all configured UDR formats in an ACS.

```
show active-charging udr-format all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging url-blacklisting statistics

Displays URL Blacklisting statistics.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging url-blacklisting statistics [ rulebase { all | name rulebase_name }
] [ verbose ] [ | { grep grep_options | more } ]
```

rulebase { all | name *rulebase_name* }

Displays URL Blacklisting statistics for all or a specific rulebase.

- **all**: Displays URL Blacklisting statistics for all configured rulebases.
- **name** *rulebase_name*: Displays URL Blacklisting statistics for the rulebase specified as an alphanumeric string of 1 through 63 characters.

verbose

Displays detailed URL Blacklisting statistics.

| { grep *grep_options* | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view URL Blacklisting hits and misses statistics.

Example

The following command displays cumulative URL Blacklisting statistics:

```
show active-charging url-blacklisting statistics
```

The following command displays URL Blacklisting statistics for the rulebase *rulebase_1*:

```
show active-charging url-blacklisting statistics rulebase name rulebase_1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show active-charging video detailed-statistics

Displays detailed statistics for TCP video flows. The command options enable you to collect statistical data for video per UE device type, per radio access type, and per video container type.

Product

MVG

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show active-charging video detailed-statistics [ container { flv | mp4 | others } | rat {
cdma | gprs | hspa | lte | others | umts | wlan } | ue { android | ios | laptop | others
} ]
```

container { flv | mp4 | others }

Displays detailed statistics for TCP video flows based on the specified container file format.

rat { cdma | gprs | hspa | lte | others | umts | wlan }

Displays detailed statistics for TCP video flows based on the specified radio access type.

ue { android | ios | laptop | others }

Displays detailed statistics for TCP video flows based on the specified UE device type.

Usage

Use this command to display detailed statistics about video usage. Use the command options to display detailed statistics based on the UE device type, radio access type, or container file format.

Example

The following command displays detailed statistics about video usage based on the UE device type *ios*:

```
show active-charging video detailed-statistics ue ios
```

show active-charging xheader-format

Displays x-header format configurations for an Active Charging Service (ACS).

Important: This is a customer-specific command. Please contact your local sales representative for more information.

Product

ACS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show active-charging xheader-format { all | name *xheader_format* **} [| { grep** *grep_options* **| more }]**

all

Displays information for all x-header formats configured.

name *xheader_format*

Displays information for the x-header format specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view details of x-header formats configured in an ACS.

Example

The following command displays information for the x-header format named *test12*:

```
show active-charging xheader-format test12
```

show administrators

Displays information regarding all CLI users currently connected to the system.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show administrators [session id] [| { grep *grep_options* **| more }]**

session id

Indicates the output is to contain additional information about the CLI user session including the assigned session ID.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

This command displays a list of administrative users that have command line interface sessions active.

Example

show administratorsshow administrators session id

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show alarm

Displays alarm information.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show alarm { all | audible | central-office | facility | outstanding [ all | chassis |
port slot/port | slot slot ] [ verbose ] | statistics } [ | { grep grep_options | more }
]
```

all

Displays the state of all alarms in one screen.

audible

Displays the state of the internal audible alarm buzzer on the SMC.

central-office

Displays the state of the CO Alarm relays on the SPIO.

facility

Displays the state of the facility (audible and CO) alarms.

outstanding [all | chassis | port *slot/port* **| slot** *slot* **] [verbose]**

Displays information on currently outstanding alarms.

- **all**: Displays all alarm information.
- **chassis**: Displays chassis/power/fan alarms.
- **port** *slot/port*: Shows the alarm information for the specified port.
- **slot** *slot*: Shows the alarm information for the card in the specified slot.
- **verbose**: Displays more verbose output, including the internal alarm ID

statistics

Displays basic statistics on the alarming subsystem, including the current number of outstanding alarms of different severities and a cumulative total of alarms generated.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command Output* section of the *Command Line Interface Overview* chapter.

Usage

View alarms to verify system status or to periodically check the general health of the system.

Important: This command is not supported on all platforms.

Example

The following command displays all alarms that are currently outstanding:

```
show alarm outstanding all
```

The following command displays more detailed information on all alarms that are currently outstanding:

```
show alarm outstanding all verbose
```

The following command displays alarm statistics:

```
show alarm statistics
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show alcap counters

Displays the Access Link Control Application Part (ALCAP) protocol message counters related to ALCAP protocol sessions associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

Product

HNB-GW

Privilege

Inspector

Syntax

show alcap counters [alcap-service *alcap_svc_name* **[aal2-node** *aal2_node_name* **[aal2-path** *aal2_path_id* **]]] [| { grep** *grep_options* **| more }]**

name *alcap_svc_name*

Specifies the name of the ALCAP service for which ALCAP protocol session counters are to be displayed.

aal2-node *aal2-node*

Specifies the name of the ATM Adaptation Layer 2 (AAL2) node for which protocol session counters will be filtered.

aal2-path *aal2_path_id*

Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node for which ALCAP protocol counters will be filtered.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter.

Usage

This command is used to display the sessions statistics and counters for ALCAP service.

Example

The following command displays the ALCAP protocol session counters for ALCAP service named as *alcap_hnb_svc1*:

```
show alcap counters alcap-service alcap_hnb_svc1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show alcap-service

Displays the Access Link Control Application Part (ALCAP) session statistics of an ALCAP service associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

Product

HNB-GW

Privilege

Inspector

Syntax

show alcap-service { all | name *alcap_svc_name* **[aal2-node** *aal2_node_name* **[aal2-path** *aal2_path_id* **[aal2-channel** *aal2_channel_num***]] | endpoint** *aal2_endpoint_name* **] } [| { grep** *grep_options* **| more }]**

name *alcap_svc_name*

Specifies the name of the ALCAP service for which service statistics are to be displayed.

aal2-node *aal2-node*

Specifies the name of the ATM Adaptation Layer 2 (AAL2) node that will be used to filter the display of the ALCAP service statistics.

aal2-path *aal2_path_id*

Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node that will be used to filter the display of the ALCAP service statistics.

aal2-channel *aal2_channel_num*

Specifies the AAL2 channel number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node that will be used to filter the display of the ALCAP service statistics.

endpoint *atm_endpoint_name*

Specifies the ATM endpoint name that will be used to filter the display of the ALCAP service statistics for a specific ATM endpoint.

Usage

This command is used to clear the sessions statistics and counters for ALCAP service.

Example

The following command displays the service statistics of ALCAP service named as *alcap_hnb_svc1*:

```
show alcap-service name alcap_hnb_svc1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show alcap statistics

Displays the session statistics related to Access Link Control Application Part (ALCAP) protocol sessions associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

Product

HNB-GW

Privilege

Inspector

Syntax

show alcap statistics [alcap-service *alcap_svc_name* **[aal2-node** *aal2_node_name* **[aal2-path** *aal2_path_id* **]]] [verbose] [| { grep** *grep_options* **| more }]**

name *alcap_svc_name*

Specifies the name of the ALCAP service for which statistics are to be displayed.

aal2-node *aal2-node*

Specifies the name of the ATM Adaptation Layer 2 (AAL2) node for which ALCAP service related statistics will be displayed.

aal2-path *aal2_path_id*

Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node for which ALCAP service statistics counters will be displayed.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter of the *Command Line Interface Reference*.

Usage

This command is used to display the sessions statistics and counters for ALCAP service.

Example

The following command displays the service session statistics counters for ALCAP service named as *alcap_hnb_svc1*:

```
show alcap counters alcap-service alcap_hnb_svc1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show apn

Displays configuration information for either a specific or all configured Access Point Names (APNs).

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show apn { all | name *apn_name* **} [| { grep** *grep_options* **| more }]**

all

Displays information on all APNs configured on the system.

name *apn_name*

Displays information for an APN specified as an alphanumeric string of 1 through 62 characters that is case sensitive.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more** options, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

This command is used to verify the configuration of one or all APNs for monitoring or troubleshooting purposes. The output is a concise listing of APN parameter settings.
If this command is executed from within the local context with the all keyword, information for all APNs configured on the system will be displayed.

Example

The following command displays configuration information for all APNs:

```
show apn all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show apn counters ip-allocation

Displays the IP allocation method information/statistics counters on per Access Point name (APN) basis for all currently active calls.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show apn counters ip-allocation [all | name *apn_name* **] [| { grep** *grep_options* **| more }]**

all

Displays statistics for all APNs.

name *apn_name*

Displays statistics for the APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

This command is used to display the IP allocation counters on per APN basis for all currently active calls. Output of this command gives the user clear idea of how many sessions in each APN are using a particular type of ip-allocation method.
If this command is issued from within the local context, the statistics displayed will be cumulative for all APNs configured on the system regardless of context. If no APN name is specified and the command is executed from a context with multiple APNs configured, the output will be cumulative for all APNs in the context.

Example

The following command displays statistics for all APN on a system:

```
show apn counter ip-allocation all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show apn statistics

Displays statistics for either a specific Access Point Name (APN) or all configured APNs.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show apn statistics [all | name *apn_name* **] [| { grep** *grep_options* **| more }]**

all

Displays statistics for all APNs.

name *apn_name*

Displays statistics for the APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

This command is used to view statistics for one or all APNs within a context for monitoring or troubleshooting purposes.
If this command is issued from within the local context, the statistics displayed will be cumulative for all APNs configured on the system regardless of context. If no APN name is specified and the command is executed from a context with multiple APNs configured, the output will be cumulative for all APNs in the context.

Example

The following command displays statistics for an APN named *isp2*:

```
show apn statistics name isp2
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show apn-profile

Displays information for configured Access Point Name (APN) profiles.

Product

MME, SGSN

Privilege

Inspector

Syntax

show apn-profile { all | full { all | name *apn_name* **} | name** *apn_name* **} [| { grep** *grep_options* **| more }]**

---

all

Lists all APN profiles configured on the system.

---

full { all | name *apn_name* **}**

full: Displays all information in the APN profile(s).
all: Displays full information for all APN profiles configured on the system.
name *apn_name*: Displays full information for an APN profile specified as an alphanumeric string of 1 through 64 characters.

---

name *apn_name*

Displays information for an APN profile specified as an alphanumeric string of 1 through 64 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information for APN profiles configured on the system. APN profiles are configured through the global configuration mode and in the APN profile configuration mode. For more information regarding APN profile commands, refer to the *APN Profile Configuration Mode Commands* chapter.

Example

The following command displays all available information for an APN profile named *apn-prof3*:

```
show apn-profile full name apn-prof3
```

show aps

Displays information for configured Automatic Protection Switching (APS) parameters.

Product

SGSN

Privilege

Inspector

Syntax

show aps { all | card-stats *slot_number* **[clear] | info** *slot_number/port_number* **| port-stats** *slot_number/port_number* **[clear] | port-status } [| { grep** *grep_options* **| more }]**

---

all

Lists APS information for all cards configured with APS.

---

card-stats*slot_number* **[clear]**

Displays the APS statistics for the identified card. If the **clear** keyword is included with the command, the APS statistics for the specified card are cleared (reset to zero).
slot_number is an integer that identifies the chassis slot holding the card.

---

info*slot_number/port_number*

Displays APS information for a specific port.
slot_number/port_number: The first number must be an integer that identifies the chassis slot holding the specified card. The slot number must be followed by a slash '/', which must be followed immediately by the port number - an integer from 1 to 4 depending upon the type of card.

---

port-stats*slot_number/port_number* **[clear]**

Displays APS statistics for a specific port. If the **clear** keyword is included with the command then the APS statistics for the specified port are cleared (reset to zero).
slot_number/port_number: The first number must be an integer from 1 to 48 to identify the chassis slot holding the specified card. The slot number must be followed by a slash '/', which must be followed immediately by the port number - an integer from 1 to 4 depending upon the type of card.

---

port-status*slot_number/port_number*

Displays APS status information for a specific port.
slot_number/port_number: The first number must be an integer from 1 to 48 to identify the chassis slot holding the specified card. The slot number must be followed by a slash '/', which must be followed immediately by the port number - an integer from 1 to 4 depending upon the type of card.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display APS redundancy configuration, APS card and port status, and APS card and port statistics. APS is configured at the card level. For details on configuring APS, refer to the *Card Configuration Mode Commands* chapter in this reference.

Important: APS is only relevant for the CLC2 and OLC2 line cards supporting SONET/SDH.

Example

The following command displays all available APS configuration information for a specific port 1 on the line card in slot 27:

```
show aps info 27/1
```

show apn-remap-table

Displays information for Access Point Name (APN) remap tables configured on the system.

Product

MME, SGSN

Privilege

Inspector

Syntax

show apn-remap-table { all | full { all | name *remap_table_name* **} | name** *remap_table_name* **} [| { grep** *grep_options* **| more }]**

all

Lists all APN remap tables configured on the system.

full { all | name *remap_table_name* **}**

full: Displays a full set (all) of available information for the configured APN remap table(s).
all: Displays the full set of available information for all APN remap tables configured on the system.
name *remap_table_name*: Displays the full set of available information for an existing APN remap table specified as alphanumeric string of 1 through 64 characters.

name *remap_table_name*

Displays information for an existing APN remap table specified as an alphanumeric string of 1 through 64 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information for APN remap tables configured on the system. APN remap tables are configured through the Global Configuration mode and in the APN remap table configuration mode. For more information regarding APN remap table commands, refer to the *APN Remap Table Configuration Mode Commands* chapter.

Example

The following command displays all available information for an APN remap table named *remap-table12*:

```
show apn-remap-table full name remap-table12
```

show asngw-service

Displays information about selected Access Service Network Gateway (ASN-GW) calls/services.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show asngw-service { all | name service_name | session | statistics } [ bs-status [
address ip_address | filter { all | icmp-monitored | no-calls | summary | up ] ] [ | {
grep grep_options | more } ]
```

---

all

Displays information for all configured ASN-GW services.

---

name *service_name*

Displays information only for an existing ASN-GW service in the current context specified as an alphanumeric string of 1 through 63 characters.

---

session

Displays information about configured ASN-GW sessions. See the **show asngw-service session** command

---

statistics

Total of collected information for specific protocol since the last **restart** or **clear** command.

---

bs-status { address *ip_address* **| filter { all | icmp-monitored | no-calls | summary | up } }**

Displays the ASN base station (BS) status based on IP address and various filters.
address *ip_address* specifies the IP address of ASN base station whose status is requested. *ip_address* must be entered in IPv4 dotted-decimal or IPv6 colon-separated notation.
filter { all | icmp-monitored | no-calls | summary | up }: Filters the requested BS's status on the basis of following criteria:

- **all**: Displays the status of all ASN base stations.
- **icmp-monitored**: Displays the status of ASN base stations that are monitored through ICMP ping messages.
- **no-calls**: Displays the status of an ASN base station that has no active calls.
- **summary**: Displays a summary of the status of requested ASN base stations.
- **up**: Displays the of status of ASN base stations that are in active state.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view information for selected configured ASN-GW services.

Example

The following command displays available information for all active ASN-GW services.

```
show asngw-service all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asngw-service session

Displays statistics for specific Access Service Network Gateway (ASN-GW) sessions.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show asngw-service session [all | anchor-only [full] | callid *call_id* **| counters | full | ip-address** *ipv4_address* **| msid** *msid_number* **| non-anchor-only [full] | peer-address** *ipv4_address* **| summary | username** *user_name* **] [| { grep** *grep_options* **| more }]**

all

Displays all related information for all active ASN-GW service sessions.

anchor-only

Displays all available information for all active ASN-GW service sessions on an anchor ASN-GW only.

callid *call_id*

Displays available information for the call identification number specified as an 8-digit hexadecimal number.

full

Displays all available information for the associated display or filter keyword.

ip-address *ipv4_address*

Specifies the IP address of the subscriber in IPv4 dotted-decimal notation.

msid *msid_number*

Displays available information for the specific mobile station identification number (MSID).

non-anchor-only

Displays all available information for all active ASN-GW service sessions on a non-anchor ASN-GW only.

peer-address *ipv4_address*

Specifies the Ip address of an IP peer in dotted-decimal notation.

summary

Displays summary of available information for associated display or filter keyword (previous keyword).

username *user_name*

Specifies the name of a user within current context as an alphanumeric string of 1 through 127 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view configuration information for an ASN-GW session.

Example

The following command displays all available ASN-GW sessions.

```
show asngw-service session all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asngw-service session counters

Displays statistics for specific Access Service Network Gateway (ASN-GW) sessions.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show asngw-service session counters [[**function-type** { **auth-relay** | **context-transfer** | **data-path** | **handoff** | **im-operation** | **ms-state-change** | **paging** | **qos** }] | [**anchor-only** | **callid** *call_id* **| ip-address** *ipv4_address* **| msid** *msid_number* | **non-anchor-only** | **peer-address** *ipv4_address* **| username** *user_name*] [**r4-only** | **r6-only** | **verbose**]] [| { **grep** *grep_options* | **more** }]

anchor-only

Displays all available information for all active anchor sessions in an ASN-GW service.

callid *call_id*

Displays available information for the call identification number specified as an 8-digit hexadecimal number.

function-type { auth-relay | context-transfer | data-path | handoff | im-operation | ms-state-change | paging | qos }

Displays the counters for specific type of functions in an ASN-GW session.
auth-relay: Displays information about authentication relay messages.
context-transfer: Displays information about context-transfer messages.
data-path: Displays information about data-path registration messages.
handoff: Displays information about hand-off messages.
im-operations: Displays information about idle mode state operation messages.
ms-state-change: Displays information about MS state change messages.
paging: Displays information about paging messages.
qos: Displays information about RR messages.

ip-address *ipv4_address*

Specifies the IP address of the subscriber in IPv4 dotted-decimal notation.

msid *msid_number*

Displays available information for the specific mobile station identification (MSID) number.

non-anchor-only

Displays all available information for all active non-anchor sessions in an ASN-GW service.

peer-address *ipv4_address*

Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.

r6-only

Displays all available counters for R6 interface in an ASN-GW session.

r4-only

Displays all available counters for R4 interface in an ASN-GW session.

username *user_name*

Displays available session information for the specific WiMAX user in ASN-GW service session.
user_name is an alphanumeric string of 1 through 127 characters.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view the counters of an ASN-GW session.

Example

The following command displays the counters for data path type function.

```
show asngw-service session counters function-type data-path
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asngw-service statistics

Displays statistics for all Access Service Network Gateway (ASN-GW) sessions.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show asngw-service statistics [function-type { auth-relay | context-transfer | data-path | handoff | im-operations | ms-state-change | paging | qos | capability }] [name *service_name* **| r4-only | r6-only | verbose | peer-address** *ipv4_address*] [**peer-id** *id*][**verbose**] [{ **grep** *grep_options* | **more** }]

function-type

Displays information about selected function type on R4 or R6 interface.

function-type { auth-relay | context-transfer | data-path | handoff | im-operations | ms-state-change | paging | qos | capability} [r4-only | r6-only]

Displays the counters for specific type of functions in an ASN-GW session.
auth-relay: Displays information about authentication relay messages.
context-transfer: Displays information about context-transfer messages.
data-path: Displays information about data-path registration messages.
handoff: Displays information about hand-off messages.
im-operations: Displays information about idle mode state operation messages.
ms-state-change: Displays information about MS state change messages.
paging: Displays information about paging messages.
qos: Displays information about RR messages.
capability: Displays the capability negotiation between the ASNGW and the base station.
r4-only: Displays information about selected function on R4 interface.
r6-only: Displays information about selected function on R6 interface.

name *service_name*

Displays information for an existing service specified as an alphanumeric string of 1 through 63 characters.

r4-only

Displays statistics of R4 interface in ASN-GW services.

r6-only

Displays statistics of R6 interface in ASN-GW services.

peer-address *ipv4_address*

Specifies the IP address of an IP Peer in IPv4 dotted-decimal notation.

peer-id < *id* >

Display the statistics based on the 6-byte BSID or ASNGW ID in addition to the IPv4 address.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { grep *grep_options* | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display ASN-GW statistics.

Example

The following command displays information about selected MS-State-Change function.

```
show asngw-service statistics function-type ms-state-change
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asnpc-service

Displays information about selected Access Service Network Paging Controller and Location Registry (ASN PC/LR) services.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show asnpc-service { all | id | name *service_name* **| session | statistics } [| { grep** *grep_options* **| more }]**

all

Displays information for all configured ASN PC services.

paging-group

Displays all the configured paging-groups and associated paging nodes, and the offset count. For a specific paging group, enter the paging group id number.

name *service_name*

Displays information only for an existing ASN PC service specified as an alphanumeric string of 1 through 63 characters.

session

Displays information about configured ASN PC sessions.

statistics

Total of collected information for specific protocol since last restart or clear command.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view information for selected configured ASN PC services.

Example

The following command displays available information for all active ASN PC services.

```
show asnpc-service all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asnpc-service session

Displays statistics for specific Access Service Network Paging Controller (ASN PC) service sessions.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show asnpc-service session [all | callid *call_id* **| counters | full | msid** *msid_number* **| peer-address** *ipv4_address* **| summary] [| { grep** *grep_options* **| more }]**

all

Displays all related information for all active ASN PC service sessions.

callid *call_id*

Displays available information for the call identification number specified as an 8-digit hexadecimal number.

full

Displays all available information for the associated display or filter keyword.

msid *msid_number*

Displays available information for the specific mobile station identification (MSID) number.

peer-address *ipv4_address*

Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.

summary

Displays summary of available information for associated display or filter keyword (previous keyword).

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view configuration information for an ASN PC session.

Example

The following command displays all available ASN PC session counters in verbose mode.

```
show asnpc-service session all
```

The following command displays full ASN PC session counters in verbose mode.

```
show asnpc-service session full
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asnpc-service session counters

Displays session counters for Access Service Network Paging Controller (ASN PC) service sessions.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show asngw-service session counters [all | callid *call_id* **| msid** *msid_number* **| peer-address** *ipv4_address* **| verbose]] [| { grep** *grep_options* **| more }]**

all

Displays all available counters for all ASN PC service sessions.

callid *call_id*

Displays available information for the call identification number specified as an 8-digit hexadecimal number.

msid *msid_number*

Displays available information for the specific mobile station identification (MSID) number.

peer-address *ipv4_address*

Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view the counters of an ASN PC session.

Example

The following command displays the counters for ASN PC service sessions in verbose mode.

```
show asnpc-service session counters verbose
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asnpc-service session counters verbose

Displays session counters for Access Service Network Paging Controller (ASN PC) service sessions in complete detail.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show asngw-service session counters verbose [function-type { context-transfer | im-operations | ms-state-change | paging }] [all | callid *call_id* **| msid** *msid_number* **| peer-address** *ipv4_address* **]] [| { grep** *grep_options* **| more }]**

---

all

Displays all available counters for all ASN PC service sessions in verbose mode.

---

callid *call_id*

Displays full information for the call identification number specified as an 8-digit hexadecimal number.

---

function-type { context-transfer | im-operations | ms-state-change | paging }

Displays the counters for specific type of functions in an ASN-GW session.
context-transfer: Displays information about context-transfer messages.
im-operations: Displays information about idle mode state operation messages.
ms-state-change: Displays information about MS state change messages.
paging: Displays information about paging messages.

---

msid *msid_number*

Displays full information for the specific mobile station identification (MSID) number.

---

peer-address *ipv4_address*

Specifies the IP address of an IP peer IPv4 dotted-decimal notation.

---

r4-only

Displays statistics of R4 interface in ASN PC services in verbose mode.

---

r6-only

Displays statistics of R6 interface in ASN PC services in verbose mode.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view the counters of an ASN PC session in verbose mode.

Example

The following command displays the counters for data path type function.

```
show asnpc-service session counters verbose
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asnpc-service statistics

Displays statistics for all ASN PC service sessions.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show asnpc-service statistics [ name service_name | peer-address ipv4_address | verbose ]
[ r4-only | r6-only [ | { grep grep_options | more } ]
```

name *service_name*

Specifies an existing service name as an alphanumeric string of 1 through 63 characters.

peer-address *ipv4_address*

Specifies the IP address of an IP Peer in IPv4 dotted-decimal notation.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display ASN PC statistics.

Example

The following command displays information about ASN PC service in verbose mode.

```
show asnpc-service statistics verbose
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show asnpc-service statistics verbose

Displays statistics for all Access Service Network Paging Controller (ASN PC) service in verbose mode.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show asnpc-service statistics verbose [ function-type { context-transfer | im-operations
| ms-state-change | paging } ] | all | r4-only | r6-only ] [ | { grep grep_options | more
} ]
```

function-type { context-transfer | ms-state-change | paging }

Displays the statistics for specific type of functions in an ASN PC service in verbose mode.
context-transfer: Displays information about context-transfer messages.
im-operations: Displays information about idle mode state operation messages.
ms-state-change: Displays information about MS state change messages.
paging: Displays information about paging messages.

all

Displays statistics of all ASN PC services in verbose mode.

r4-only

Displays statistics of R4 interface in ASN PC services.

r6-only

Displays statistics of R6 interface in ASN PC services.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display ASN PC service statistics in verbose mode.

Example

The following command displays information about selected MS-State-Change function.

```
show asnpc-service statistics verbose function-type ms-state-change
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show banner

Displays the configured banner message for the current context.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show banner { all | charging-service | motd | lawful-intercept | pre-login } [| { grep *grep_options* **| more }]**

all

Displays all banners configured for a service in a system including the enhanced charging service (ECS).

charging-service

Displays banner message configured for an enhanced charging service in the current context.

motd

Display the banner message that is configured for the current context.

lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Show the configured banner to verify the message of the day contents for possible change

Example

```
show banner
```

show bcmcs counters

Displays Broadcast and Multicast Service (BCMCS)-specific counters and statistics.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show bcmcs counters { all | callid *call_id* **| flow-id** *flow_id* **}**

all

Displays BCMCS-specific counters and statistics for all multicast sessions.

callid *call_id*

Displays BCMCS-specific counters and statistics for a specific call ID.

flow_id *flow_id*

Displays BCMCS-specific counters and statistics for a specific BCMCS flow, defined by a flow ID.

Usage

Use this command to view BCMCS-specific statistics. You may narrow the results of the command output by specifying a specific call ID or flow ID.

Example

```
show bcmcs counters all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show bcmcs statistics

Displays Broadcast and Multicast Service (BCMCS)-specific statistics for the current PDSN-service.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show bcmcs statistics [pdsn-service *service_name* **]**

pdsn-service *service_name*

Defines a specific PDSN service from which to gather BCMCS-specific statistics.

Usage

Shows several sets of BCMCS-specific statistics, and may be configured to show statistics only for a certain PDSN service.

Example

show bcmcs statistics pdsn-service *service_name*

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show boot

Displays information on the current boot image in use.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show boot [initial-config | { grep *grep_options* **| more }]**

initial-config

Identifies the OS image, configuration file, and boot priority used during the initial start up of the system.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Show the boot information in preparing for maintenance activities by verifying current boot data. The boot image in use may not be the same as the boot image stored on the SMC due to upgrades and pending reboots. **show boot initial-config** displays the actual boot image and configuration file loaded during boot. This may or may not be the highest priority image and makes this command useful when comparing the loaded image to the priority list.

Important: This command is not supported on all platforms.

Example

The following command displays the boot system configuration priority list:

```
show boot
```

The following command displays the initial configuration after a system boot:

```
show boot initial-config
```

show bssap+ statistics

Displays Base Station system Application Part (BSSAP+) protocol statistics for the Gs interface between the SGSN and the Mobile services Switching Centre, Visitor Location Register (MSC/VLR).

Product

SGSN

Privilege

Inspector

Syntax

show bssap+ statistics [gs-service *gs_svc_name* **] [vlr { isdn-number** *ISDN_Num*| **name** *vlr_name* **}] [verbose] [| { grep** *grep_options* **| more }]**

gs-service *gs_svc_name*

Specifies the name of a specific Gs service to filter the BSSAP+ information as an alphanumeric string of 1 through 63 characters that is case sensitive.

vlr { isdn-number *ISDN_Num*| **name** *vlr_name*

Identifies a specific VLR (by name or ISDN number) to filter BSSAP+ information.
vlr_name is the configured name of the VLR expressed.
VLR_num is the configured E.164-type ISDN number for the VLR. Enter a numerical string of 1 to 15 digits.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be limited to a concise summary.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display the BSSAP+ statistics for the SGSN's Gs interface(s). Based on how the command is entered, this command displays collected BSSAP+ protocol statistics for the entire SGSN or for a specified Gs interface. Using the keywords of this command, the interface can be identified by defining a specific VLR connected to the SGSN or by identifying the Gs service to which the interface has been configured.

Example

The following command displays all BSSAP+ information for the Gs interface configured for the Gs service named *gssvc1*.

```
show bssap+ statistics gs-service gssvc1 verbose
```

Important: Descriptions for show command outputs are available in the **Statistics and Counters Reference**.

show bssgp statistics

Displays base station subsystem GPRS protocol statistics for traffic between the base station subsystem (BSS) and the SGSN over the Gb interface.

Product

SGSN

Privilege

Inspector

Syntax

show bssgp statistics [gprs-service *gprs_svc_name* **| nse** *nse_id* **[bvc** *bvc_id* **[sessmgr | verbose]]] [verbose] [| { grep** *grep_options* **| more }]**

gprs-service *gprs_svc_name*

Specifies the name of an existing GPRS service for which the BSSGP information will be filtered as an alphanumeric string of 1 through 63 characters that is case-sensitive.

nse*nse_ID*

Enter this keyword to display the BSSGP statistics for the network service entity (NSE) specified as an integer from 0 through 65535.

bvc*bvc_ID*

Enter this keyword to display the BSSGP statistics for the BSSGP virtual connection (BVC) specified as an integer from 0 through 6500.

sessmgr instance *sessmgr_instance*

Enter this keyword to display the BSSGP statistics for a session manager instance specified as an integer from 1 through 4294967295.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display the BBSGP statistics for a particular GPRS service or NSEI.

Example

The following command displays BSSGP statistics for the GPRS service named *gprs1*.

```
show bssgp statistics gprs-service gprs1
```

Important: Descriptions for show command outputs are available in the **Statistics and Counters Reference**.

show bssgp status

Displays the traffic status through the BSSGP (base station subsystem GPRS protocol) layer between the base station subsystem (BSS) and the SGSN over the Gb interface.

Product

SGSN

Privilege

Inspector

Syntax

show bssgp status { bvc-bucket nsei *nse_id* **bvci** *bvc_id* **| bvc-stat nsei** *nse_id* **bvci** *bvc_id* **} [| { grep** *grep_options* **| more }]**

bvc-bucket nsei*nse_id* **bvci** *bvc_id*

Displays traffic status for a specific BVC bucket identified by the NSEI (network service entity ID) and BVCI (BSSGP virtual connection ID).
nse_ID is an integer from 0 through 65535.
bvc_ID is an integer from 0 through 65000.

bvc-stat nsei*nse_id* **bvci** *bvc_id*

Displays traffic status for a BVC identified by the NSEI (network service entity ID) and BVCI (BSSGP virtual connection ID).
nse_ID is an integer from 0 through 65535.
bvc_ID is an integer from 0 through 65000.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display BVC status of the BBSGP layer for specified NSEI and BVCI.

Example

The following command displays BSSGP traffic status for the BVC bucket for NSEI *2556* BVCI *241*.

```
show bssgp status bvc-bucket nsei 2556 bvci 241
```

Important: Descriptions for show command outputs are available in the **Statistics and Counters Reference**.

show bulkstats

Displays the information on bulk statistics.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show bulkstats [[data] | [schemas] | [variables [*schema_name* **] [obsolete]] [| { grep** *grep_options* **| more }]]**

data

Displays collected bulk statistical data.

schema

Displays the configuration of the statistics to be collected on a per-schema basis.

Important: For information on available schemas, refer to the *Bulk Statistics Configuration Mode Commands* chapter.

variables *schema_name*

Displays all valid bulkstat schema statistics, or only the statistics for the specified schema. *schema_name* specifies the name of the schemas available on system. The following is the list of available schemas in this release.

- aal2
- alcap
- apn
- asngw
- asnpc
- bcmcs
- card
- closedrp
- common
- context
- cs-network-ranap
- cs-network-rtp
- cscf
- cscfintf

- dcca
- diameter-acct
- diameter-auth
- diameter-acct
- dlci-util
- dpca
- ecs
- egtpc
- epdg
- fa
- fng
- gprs
- gtpc
- gtpp
- gtpu
- ha
- hnbgw-hnbap
- hnbgw-ranap
- hnbgw-rtp
- hnbgw-rua
- hnbgw-sctp
- hsgw
- imsa
- ippool
- ipsg
- lac
- lma
- lns
- mag
- map
- mipv6ha
- mme
- mvs
- nat-realm

- pcc-af
- pcc-policy
- pcc-service
- pcc-sp-endpt
- pdg
- pdif
- pgw
- phsgw
- phspc
- port
- ppp
- ps-network-ranap
- radius
- rp
- sccp
- sgs
- sgsn
- sgtp
- sgw
- ss7link
- ss7rd
- system
- vpn

obsolete

This keyword shows the obsolete (but still available) schema variables. An asterisk (*) is displayed next to schema variables that have been obsoleted.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For information on usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

This command is used to display information on bulk statistics supported by the system.
The **variable** keyword can be used to list statistics supported by the system either for all schemas, or for an individual schema.

The **schema** keyword can be used to display the configuration of settings for bulk statistics, including the schema.
The **data** keyword can be used to display bulk statistic data collected up to that point.

Example

The following command displays the bulk statistics data:

```
show bulkstats data
```

The following command displays the bulk statistics schema configuration:

```
show bulkstats data schemas
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ca-certificate

Displays information for Certificate Authority (CA) digital certificates on this system.

Product

All

Privilege

Inspector

Syntax

show ca-certificate { all | name *name* **}**

all

Displays CA certificate information for all CA certificates known to this system.

name *name*

Displays CA certificate information for an existing CA certificate name specified as n alphanumeric string of 1 through 128 characters.

Usage

View information for CA certificates on this system.

Example

The following command displays information for a CA certificate named *cert-1*:

```
show ca-certificate name cert-1
```

Important: Output descriptions for some commands are available in the *Statistics and Counters Reference*.

show ca-crl

Displays information for Certificate Authority (CA) Certificate Revocation List (CRL) on this system.

Product

All

Privilege

Inspector

Syntax

show ca-crl { all | name *name* **}**

all

Displays CA-CRL information for all CA-CRLs known to this system.

name *name*

Displays CA-CRL information for an existing CA-CRL name specified as an alphanumeric string of 1 through 128 characters.

Usage

View information for CA-CRLs on this system.

Example

The following command displays information for a CA-CRL named *crl-5*:

```
show ca-crl name crl-5
```

Important: Output descriptions for some commands are available in the *Statistics and Counters Reference*.

show cae-group server

Displays configuration information, including the name of the associated CAE group, for all CAEs or for a specific CAE. The CAE (Content Adaptation Engine) is an optional component of the Mobile Videoscape.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

show cae-group server { all | name *cae_name* **}**

all

Shows the configuration information, including the associated CAE group, for all CAEs.

name *cae_name*

Shows the configuration information for a specific CAE.

Usage

Use this command to display configuration information for all CAEs or for a specific CAE. This command can be issued from either the local context or the context in which the associated CAE group is defined.

Example

The following command displays configuration information for the CAE named *server_1*:

```
show cae-group server name server_1
```

show call-control-profile

Displays information for call control profiles configured on the system.

Product

MME, SGSN

Privilege

Inspector

Syntax

```
show call-control-profile { all | full { all | name profile_name } | name profile_name }
[ | { grep grep_options | more } ]
```

all

Lists all call-control profiles configured on the system.

full { all | name *profile_name* **}**

full: Displays a full set (all) of available information in the call-control profile.
all: Displays a full set of available information for all call-control profiles configured on the system.
name *profile_name*: Displays full information for an existing call-control profile specified as an alphanumeric string of 1 through 64 characters.

name *profile_name*

Displays information for an existing call-control profile specified as an alphanumeric string of 1 through 64 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information for call-control profiles configured on the system. Call-control profiles are configured through the global configuration mode and in the call-control profile configuration mode. For more information regarding call-control profile commands, refer to the *Call-Control Profile Configuration Mode Commands* chapter.

Example

The following command displays all available information for a call-control profile named *call-prof2*:

```
show call-control-profile full name call-prof2
```

show call-home

Displays information for Smart Call Home settings configured on the system.

Product

All

Privilege

Security Administrator, Administrator

Syntax

show call-home [alert-group | detail | mail-server status | profile [all | name *profile_name* **] | statistics [| { grep** *grep_options* **| more }]]**

alert-group

Displays information for all alert groups configured on the system. It also indicates if an alert-group has been disabled by the user.

detail

Displays general information and alert-group settings for all configured call-home profiles.

mail-server status

Displays status information for call-home mail servers that are configured on the system.

profile { all | name *profile_name* **}**

Displays all available information for all call-home profiles on the system or a specified call-home profile.
all: Displays all available information for all call-home profiles configured on the system.
name *profile_name*: Displays all available information for an existing call-home profile specified as an alphanumeric string of 1 through 31 characters.

name *profile_name*

Displays information for a call-home profile specified as an alphanumeric string of 1 through 31 characters.

statistics

Displays statistical information for call-home statistics configured on the system.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display profile and notification policy information associated with the call-home profiles configured on the system. Call-home profiles are configured through the Context Configuration

Mode and in the Call-home Configuration Mode. For more information regarding call-home commands, refer to the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command displays all available information for a call-home profile named *call-home-prof1*:

```
show call-home profile name call-home-prof1
```

show call-control-profile

Displays information for call control profiles configured on the system.

Product

MME, SGSN

Privilege

Inspector

Syntax

```
show call-control-profile { all | full { all | name profile_name } | name profile_name }
[ | { grep grep_options | more } ]
```

all

Lists all call-control profiles configured on the system.

full { all | name *profile_name* **}**

full: Displays all available information in the call-control profile.
all: Displays a full set of available information for all call-control profiles configured on the system.
name *profile_name*: Displays a full set of available information for a an existing call-control profile specified as an alphanumeric string of 1 through 64 characters.

name *profile_name*

Displays information for an existing call-control profile specified as an alphanumeric string of 1 through 64 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information for call-control profiles configured on the system. Call-control profiles are configured through the global configuration mode and in the call-control profile configuration mode. For more information regarding call-control profile commands, refer to the *Call-Control Profile Configuration Mode Commands* chapter in this reference.

Example

The following command displays all available information for a call-control profile named *call-prof2*:

```
show call-control-profile full name call-prof2
```

show camel-service

Displays configuration details for Customized Applications for Mobile networks Enhanced Logic (CAMEL) services configured for this SGSN.

Product

SGSN

Privilege

Inspector

Syntax

show camel-service { all | name *service_name* **} [| grep** *grep_options* **| more]**

all

Displays the configuration details for all configured CAMEL services.

name

Displays the configuration details for an existing CAMEL service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View configuration information for CAMEL services.

Example

The following command displays the configuration information for a CAMEL service identified as *camel4sgsnTO*:

```
show camel-service name camel4sgsnTO
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show certificate

Displays information for local node certificates configured on this system.

Product

All

Privilege

Inspector

Syntax

```
show certificate { all | name name }
```

all

Displays certificate information for all node certificates configured on this system.

name *name*

Displays information for a certificate name specified as an existing certificate name expressed as an alphanumeric string of 1 through 128 characters.

Usage

View information for local node certificates on this system.

Example

The following command displays information for a node certificate named *certificate-3*:

```
show certificate name certificate-3
```

Important: Output descriptions for some commands are available in the *Statistics and Counters Reference*.

show cli

Displays current command line interface (CLI) users and associated session information.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show cli { session | history } [| { grep *grep_options* **| more }]**

session

Displays information about the current CLI session.

history

Displays CLI command history for this CLI session.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Show current command line interface sessions when there is some unexpected output from a chassis and a check of current CLI users may reveal other activities in progress.

Example

```
show cli
```

show clock

Displays the current system data and time.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show clock [universal] [| { grep *grep_options* **| more }]**

universal

Displays the date and time in universal coordinated time (UTC/GMT) format.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command Output* section of the *Command Line Interface Overview* chapter.

Usage

Check the current time of a chassis to compare with network wide time or for logging purposes if network accounting and/or event records appear to have inconsistent timestamps.

Important: This command is not supported on all platforms.

Example

The following displays the system time in local time and UTC, respectively.

```
show clock

show clock universal
```

show configuration

Displays current configuration information for various subcomponents of the system.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

show configuration [card *card_num* **| checksum | context** *name* **| obsolete-encryption | port** *slot/port* **| rohc | showsecrets | srp | url** *url* **| verbose] [| { grep** *grep_options* **| more }]**

show configuration card *card_num* **[obsolete-encryption | showsecrets | verbose]**

show configuration checksum [obsolete-encryption | showsecrets | verbose]

show configuration context *name* **[obsolete-encryption | showsecrets | verbose]**

show configuration obsolete-encryption

show configuration port *slot/port* **[obsolete-encryption | showsecrets | verbose]**

show configuration rohc [all | profile-name *name* **] [verbose]**

show configuration showsecrets [obsolete-encryption]

show configuration srp [checksum [obsolete-encrpytion] | showsecrets [obsolete-encrption] | verbose]

show configuration url *url*

show configuration verbose [obsolete-encrpytion | showsecrets [obsolete-encrption]]

---

card *card_num* **[obsolete-encryption | showsecrets | verbose]**

Specifies a card for which configuration information is to be displayed as an integer from 1 through 48. Additional display options include:

- **obsolete-encryption**: Shows encrypted values using a weaker, obsolete encryption method.
- **showsecrets**: Shows unencrytpted secrets
- **verbose**: Shows all available details.

checksum [obsolete-encryption | showsecrets | verbose]

Generates and displays a checksum value for the configuration data.

Additional display options include:

- **obsolete-encryption**: Shows encrypted values using a weaker, obsolete encryption method.
- **showsecrets**: Shows unencrytpted secrets
- **verbose**: Shows all available details.

context *name* **[obsolete-encryption | showsecrets | verbose]**
Specifies an existing context for which configuration information is to be displayed as an alphanumeric string of 1 through 79 characters.

Additional display options include:

- **obsolete-encryption**: Shows encrypted values using a weaker, obsolete encryption method.
- **showsecrets**: Shows unencrytpted secrets
- **verbose**: Shows all available details.

obsolete-encryption
Shows encrypted values using a weaker, obsolete encryption method.

port *slot/port* **[obsolete-encryption | showsecrets | verbose]**
Displays configuration information for a port identified by its slot and port numbers.

Additional display options include:

- **obsolete-encryption**: Shows encrypted values using a weaker, obsolete encryption method.
- **showsecrets**: Shows unencrytpted secrets
- **verbose**: Shows all available details.

rohc [all | profile-name *name* **] [verbose]**
Specifies that information for all robust header compression (RoHC) profiles or the named profile is to be displayed.

Additional display option includes:

- **verbose**: Shows all available details.

showsecrets [obsolete-encryption]
Shows encrypted and unencrytpted secret keys saved in the configuration. If this keyword is not specified, secret keys are not displayed.

Additional display option includes:

- **obsolete-encryption**: Shows encrypted values using a weaker, obsolete encryption method.

---

srp [checksum [obsolete-encrpytion] | showsecrets [obsolete-encrption] | verbose]

Shows the Service Redundancy Protocol (SRP) configuration.
checksum [obsolete-encryption]: Displays checksum information with the option to display encrypted values using a weaker obsolete encryption method.
showsecrets [obsolete-encrption]: Displays unencrytpted secrets with the option to display encrypted values using a weaker obsolete encryption method.
Additional display option includes:
- **verbose**: Shows all available details.

---

url *url*

Default: configuration which is currently in use.
This keyword is not available to users with Operator level permissions. Specifies the location of the configuration data to use for information display. The *url* may refer to a local or a remote file and must be entered in the following format:
[file:]{ /flash | /pcmcia1 | /hd }[/*directory* **]/***file_name*
tftp://{ *host***[** *:port#* **] }[/***directory* **]/***file_name*

[http: | ftp: | sftp:]//[*username***[** *:password* **]@] { ***host* **}[** *:port#* **][/***directory* **]/***file_name*

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.
filename is the actual file of interest.

Important: Configuration files should be named with a **.cfg** extension.

username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View the current configuration to review recent changes.

Important: This command is not supported on all platforms.

Example

The following command displays the local in-use port configuration information for port *24/1* in verbose mode.

```
show configuration port 24/1 verbose
```

The following command displays the card configuration for card *17* on host *remoteABC* stored in the configuration file in */pub/config.cfg*.

```
show configuration card 17
```

The following command displays the card configuration for card *5* on host *remoteABC* stored in the configuration file in */pub/config.cfg*.

```
show configuration card 5
```

The following command displays the configuration of all RADIUS server groups configured in context *local*

```
show configuration context local radius group all
```

The following command shows the configuration for a context named PDIF.

```
show configuration context pdif
```

show configuration errors

Displays current configuration errors and warning information for the target configuration file as specified for a service.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

show configuration errors [section *section_name* **] [verbose] [| { grep** *grep_options* **| more }]**

---

section {*section_name***}**

Specifies the services and section for which to display and validate a configuration.
The following services and sections are supported:

- **aaa-config**: Displays configuration errors/warnings for the AAA service(s) configured on the system.
- **active-charging**: Displays configuration errors/warnings for the Enhanced Charging Service(s) and the Personal Stateful Firewall service(s) configured on the system.
- **apn**: Displays configuration errors/warnings for the APN configuration(s) on the system.
- **apn-profile**: Displays configuration errors/warnings for the APN Profile configuration(s) on the system.
- **apn-remap-table**: Displays configuration errors/warnings for the APN Remap Table configuration(s) on the system.
- **asngw-service**: Displays configuration errors/warnings for the Access Service Network Gateway (ASN-GW) Service configured in a specific context for which configuration errors/warnings is to be displayed.
- **asnpc-service**: Displays configuration errors/warnings for the ASN Paging Controller and Location Registry (ASN PC-LR) Service(s) configured on the system.
- **call-control-profile**: Displays configuration errors/warnings for the Call Control Profile configuration(s) on the system.
- **camel-service**: Displays configuration errors/warnings for the CAMEL Service configuration(s) on the system.
- **closed-rp-service**: Displays configuration errors/warnings for the closed RP service(s) configured on the system.
- **cs-network**: Displays configuration errors/warnings for the CS Network configuration(s) on the system.
- **cscf-service**: Displays configuration errors/warnings for the Call Session Control Function (CSCF) service(s) configured on the system.
- **diameter**: Displays configuration errors/warnings for the Diameter configuration(s) on the system.
- **dns-client**: Displays configuration errors/warnings for the DNS Client configuration(s) on the system.

- **egtp-service**: Displays configuration errors/warnings for the eGTP Service configuration(s) on the system.
- **event-notif**: Displays configuration errors/warnings for the event notification (SNMP) interface client.
- **fa-service**: Displays configuration errors/warnings for the Foreign Agent (FA) service(s) configured on the system.
- **fng-service**: Displays configuration errors/warnings for the Femto Network Gateway (FNG) configuration(s) on the system.
- **ggsn-service**: Displays configuration errors/warnings for the GGSN service(s) configured on the system.
- **gprs-service**: Displays configuration errors/warnings for the GPRS service(s) configured on the system.
- **gs-service**: Displays configuration errors/warnings for the GS service(s) configured on the system.
- **ha-service**: Displays configuration errors/warnings for the Home Agent (HA) service(s) configured on the system.
- **hnbgw-service**: Displays configuration errors/warnings for the Home Evolved Node B Gateway (HNB-GW) Service configuration(s) on the system.
- **hsgw-service**: Displays configuration errors/warnings for the HRPD Serving Gateway (HSGW) service(s) configured on the system.
- **imei-profile**: Displays configuration errors/warnings for the International Mobile Equipment Identity (IMEI) Profile configuration(s) on the system.
- **imsa-config**: Displays configuration errors/warnings for the IMS Authorization (IMSA) configuration(s) on the system.
- **imssh-service**: Displays configuration errors/warnings for the IMS Sh (IMSSh) service(s) configured on the system.
- **imsue-service**: Displays configuration errors/warnings for the IMS UE service(s) configured on the system.
- **ipms**: Displays configuration errors/warnings for the Intelligent Packet Monitoring System (IPMS) service(s) configured on the system.
- **ipsg-service**: Displays configuration errors/warnings for the IP Security Gateway (IPSG) service(s) configured on the system.
- **iups-service**: Displays configuration errors/warnings for the IuPS service(s) configured on the system.
- **lac-service**: Displays configuration errors/warnings for the Layer 2 Tunneling Protocol (L2TP) Access Concentrator (LAC) service(s) configured on the system.
- **lns-service**: Displays configuration errors/warnings for the L2TP Network Server (LNS) service(s) configured on the system.
- **local-policy**: Displays configuration errors/warnings for the Local Policy configuration(s) on the system.
- **map-service**: Displays configuration errors/warnings for the SS7 Mobile Application Part (MAP) service(s) configured on the system.

- **mme-service**: Specifies the configuration errors for a Mobility Management Entity (MME) service configured in a specific context for which configuration errors/warnings are to be displayed.
- **operator-policy**: Displays configuration errors/warnings for the Operator Policy configuration(s) on the system.
- **pcc-policy-service**: Displays configuration errors/warnings for the Policy and Charging Control (PCC) Policy Service configuration(s) on the system.
- **pcc-service**: Displays configuration errors/warnings for the PCC Service configuration(s) on the system.
- **pdg-service**: Displays configuration errors/warnings for the Packet Data Gateway (PDG) Service configuration(s) on the system.
- **pdif-service**: Displays configuration errors/warnings for the Packet Data Interworking Function (PDIF) service(s) configured on the system.
- **pdsn-service**: Displays configuration errors/warnings for the PDSN service(s) configured on the system.
- **pgw-service**: Displays configuration errors/warnings for the P-GW Service configuration(s) on the system.
- **phsgw-service**: Displays configuration errors/warnings for the PHS Gateway service(s) configured on the system.
- **policy-grp-config**: Displays configuration errors/warnings for the Policy Group configuration(s) on the system.
- **ps-network**: Displays configuration errors/warnings for the PS Network configuration(s) on the system.
- **sccp-network**: Displays configuration errors/warnings for the SCCP network configuration(s) on the system.
- **sgs-service**: Displays configuration errors/warnings for the SGs Service configuration(s) on the system.
- **sgsn-mode**: Displays configuration errors/warnings for the SGSN Mode configuration(s) on the system.
- **sgsn-service**: Displays configuration errors/warnings for the SGSN service(s) configured on the system.
- **sgtp-service**: Displays configuration errors/warnings for the SGSN GPRS Tunneling Protocol (SGTP) service(s) configured on the system.
- **sgw-service**: Displays configuration errors/warnings for the S-GW Service configuration(s) on the system.
- **subscriber-config**: Displays configuration errors/warnings for the Subscriber configuration(s) on the system.
- **subscriber-map**: Displays configuration errors/warnings for the Subscriber Map configuration(s) on the system.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For more information on the usage of **grep** and **more**, refer *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view the current configuration errors and warning to review recent changes.

Example

The following command displays configuration errors and warnings for all services configured in a context/system:

```
show configuration errors verbose | more
```

The following command displays configuration errors and warnings for Enhanced Charging service and Personal Stateful Firewall service configured in a context:

```
show configuration errors section active-charging verbose
```

show congestion-control

Displays information pertaining to congestion control functionality on the system

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show congestion-control {**configuration** | **statistics** {*demux_mgr* } [**all** | **instance** *task_instance*] } [| { **grep** *grep_options* | **more** }]

configuration

Displays congestion control configuration information including threshold parameters and policy settings for the configured services.

statistics

Displays congestion control statistics for Demux managers *demux_mgr*.
all: Displays statistics based on the current state of all instances of the specified task.
instance *task_instance*: Displays statistics for a software task instance specified as an integer from 1 through 128. 8.

Important: The **inst** column of the **show task table** command output displays the instance of a particular task.

demux_mgr

Specifies the name of the service/session Demux manager for which statistics are displayed. The following types of *demux_mgr* services are supported:

- **a11mgr**: Specifies that statistics are displayed for PDSN services.
- **asngwmgr**: Specifies that statistics are displayed for ASN-GW services.
- **asnpcmgr**: Specifies that statistics are displayed for ASN PC-LR services.
- **bindmux**: Specifies that statistics are displayed for Bindmux Manager used by PCC service.
- **egtpinmgr**: Specifies that statistics are displayed for EGTP ingress demuxmgr.
- **gtpcmgr**: Specifies that statistics are displayed for GGSN services.
- **hamgr**: Specifies that statistics are displayed for HA services.
- **hnbmgr**: Specifies that statistics are displayed for HNB Manager used by HNB-GW service.
- **imsimgr**: Specifies that statistics are displayed for IMSI managers.
- **ipsecmgr**: Specifies that statistics are displayed for IPSec managers.
- **l2tpmgr**: Specifies that statistics are displayed for L2TP managers.

all

Displays the statistics based on the current state of all instances of the specified task.

instance *task_instance*

Displays statistics for a specified software task instance. *task_instance* can be configured to an integer from 1 to 128.

Important: The **inst** column of the **show task table** command output displays the instance of a particular task.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

This command displays congestion control configuration information or statistics for a particular service type. When the all keyword is used, the system compares the current state of all instances of the specified task. The state is based on whether or not any congestion control thresholds have been exceeded. If one or more instances are experiencing congestion, the state is displayed as "Applied", and the various thresholds that have been crossed are indicated.

Example

The following command displays congestion control statistics for a PDSN service using an **a11mgr** task with an instance of *2*:

```
show congestion-control statistics a11mgr instance 2
```

The following command displays congestion control statistics for an ASN-GW service using an **asngwmgr** task with an instance of *2*:

```
show congestion-control statistics asngwmgr instance 2
```

The following command displays congestion control statistics for an ASN PC-LR service using an **asnpcmgr** task with an instance of *2*:

```
show congestion-control statistics asnpcmgr instance 2
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show content-filtering category database

Displays details of the specified category based content filtering database for content filtering application configured in a system/service.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show content-filtering category database [active | all | facility srdbmgr { all | instance *instance_value* **} | url** *url_string* **] [verbose] [| { grep** *grep_options* **| more }]**

active

Displays the information about all active databases, for example databases in memory. This is the default setting for category database information.

all

Displays the information about all active databases, for example, databases in memory and all saved databases on a system.

facility

Displays logged events for a specific facility.

srdbmgr { all | instance *instance_value* **}**

Displays logged events for all static rating database managers or for all or for a specific instance.

- **all**: Displays the logged events for all Static Rating Database (SRDB) Manager instances.
- **instance** *instance_value*: Displays events logged for a specific SRDB Manager instance specified as an integer from 1 through 8.

url *url_string*

Displays the information of the database located at the URL that specifies the name/location of the category database from which to retrieve information as an alphanumeric string of 1 through 512 characters.

verbose

This option enables the detailed mode for additional information display for specific database.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information of database for category based content filtering application in a service.

Example

The following command displays a detailed information for all active databases in memory.

```
show content-filtering category database active all
```

The following command displays the CF database status of all running SRDB managers.

```
show content-filtering category database facility srdbmgr all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show content-filtering category policy-id

Displays Content Filtering category policy definitions.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show content-filtering category policy-id { all | id *cf_policy_id* **} [| { grep** *grep_options* **| more }]**

all

Displays definitions of all Content Filtering category policies.

id *cf_policy_id*

Displays definitions of an existing Content Filtering category policy ID specified as an integer from 1 through 4294967295.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view Content-Filtering Category definitions for a specific/all Policy IDs.

Example

The following command displays Content Filtering category definitions for policy ID *3*:

```
show content-filtering category policy-id id 3
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show content-filtering category statistics

Displays statistics for the category-based Content Filtering application configured in a system/service.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show content-filtering category statistics [ facility srdbmgr { all | instance
instance_value } ] [ | { grep grep_options | more } ]
```

facility

Displays logged events for a specific facility.

srdbmgr { all | instance *instance_value* }

Displays logged events for all Static Rating Database (SRDB) Manager instances or for the specified instance.

- **all**: Displays events logged for all SRDB Manager instances.
- **instance** *instance_value*: Displays events logged for the SRDB Manager instance specified as an integer from 1 through 8.

| { grep *grep_options* | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view the statistics of Category Based Content Filtering application in a service. This command's output also indicates capability of the system to perform Content Filtering and Dynamic Content Filtering if configured.

Important: Content filtering cannot be performed if less than two PSCs are activated. Dynamic Content Filtering cannot be performed if less than three PSCs are activated.

Example

The following command displays the detailed statistics of configured category based content filtering application:

```
show content-filtering category statistics
```

The following command displays the detailed statistics of configured category based content filtering application based on running SRDB Manager *instance1*.

```
show content-filtering category statistics facility srdbmgr instance
instance1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show content-filtering category url

Displays the information about the categories of the database at the specific URL configured for the category-based content filtering application in a system/service.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show content-filtering category url *url_string* **[policy-id** *cf_policy_id* **| rulebase** *rulebase_name* **] [verbose] [| { grep** *grep_options* **| more }]**

url *url_string*

Displays the category information of the URL specified as an alphanumeric string of 1 through 512 characters.

policy-id *cf_policy_id*

Displays the category information of a URL configured with an existing content filtering category policy ID specified as n integer from 0 through 65535.

rulebase *rulebase_name*

Displays the category information of a URL configured in ACS Configuration Mode for category-based content filtering in specific rulebase. *rulebase_name* must be the name of an existing rulebase expressed as an alphanumeric string of 1 through 15 characters.

verbose

Enables the detailed mode for additional information display for a specific database.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information of a database URL for category based content filtering application in a service.

Example

The following command displays a detailed information for all active databases in memory.

```
show content-filtering category url /cf_server/cf/optcmd.bin verbose
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show content-filtering server-group

Displays information for Content Filtering Server Group (CFSG) configured in the service.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show content-filtering server-group [name *cfsg_name* **| statistics] | [| { grep** *grep_options* **| more }]**

name *cfsg_name*

Displays information for an existing CFSG specified as an alphanumeric string of 1 through 63 characters.

statistics

Displays statistical information for all configured CFSGs.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information for Content Filtering Server Group configured in a service.

Example

The following command displays a detailed information for all charging actions:

```
show content-filtering server-group statistics
```

The following command displays a details of a specific charging action:

```
show content-filtering server-group name test123
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show context

Displays information for currently configured contexts.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show context [ all | name context_name ] [ | { grep grep_options | more } ]
```

all | name *context_name*

all: Displays information for all currently configured contexts.
name *context_name*: Displays information for an existing context specified as an alphanumeric string of 1 through 79 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View configured contexts. This may be useful in verifying configuration or troubleshooting the system.

Example

The following command displays information for the configured context named *sampleContext*:

```
show context name sampleContext
```

The following command displays information for all contexts:

```
show context all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cpu

Displays information on system CPUs.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show cpu { info [card *card_num* **[cpu** *cpu_num* **]] [graphs] [verbose] | table } [| { grep** *grep_options* **| more }]**

---

info [card *card_num* **[cpu** *cpu_num* **]] [graphs] [verbose]**

Displays information for an entire card or a specific CPU.
card *card_num*: Specifies the card for which to display associated information. *card_num* must be a value in the range 1 through 48 and must refer to an installed card.
cpu *cpu_num*: Optionally selects a specific CPU on the card of interest to display specific information. *cpu_num* must be a value in the range 0 through 3 and must refer to an installed CPU.
graphs: In addition to textual CPU information display CPU utilization information in graphs.
verbose: Output is to display all information available.

---

table

Display, in tabular format, all cards and CPUs.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View CPU statistics to aid in diagnosing service problems for the case of overload conditions.

Important: This command is not supported on all platforms.

Example

The following command displays the CPU information in tabular format for all CPUs on all installed cards:

```
show cpu table
```

The following command displays CPU information for card *8* in verbose mode:

```
show cpu info card 8 verbose
```

The following command displays information for CPU *0* on card *1*:

```
show cpu info card 1 cpu 0
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show crash

Displays summary of system/task crashes or information on a specific crash.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show crash { list | number *crash_num* **} [| { grep** *grep_options* **| more }]**

list | number *crash_num*

list: Displays a list of recent crash data.
number *crash_num* displays the information for an existing crash number. The crash number can be displayed using the **list** keyword.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

VIew the crash list to determine frequency of crashes or if crashes occur at some specific time of day. This may also be used to view information on a specific crash to aid in troubleshooting.

Example

The following displays the list of recent crashes.

```
show crash list
```

The following command will display the crash information for crash number *11*.

```
show crash number 11
```

show credit-control sessions

Displays credit control sessions information.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show credit-control session [all | callid | full | mdn | nai | summary] [| { grep *grep_options* **| more }]**

---

session [all | callid | full | mdn | nai | summary]

Displays the credit control session status based on the following keywords:
all: Displays all available information for Credit Control sessions
callid: Displays the Credit Control Session Call ID
full: Displays All available information for the associated display or the filter keyword
mdn: Displays the Credit Control Message Delivery Notification (MDN) information.
nai: Displays the Credit Control NI
summary: Displays the summary of Credit Control session information

---

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Please refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage

Use this command to show active credit control application for service sessions.

Example

The following command shows the configured Credit Control application sessions:

```
show credit-control sessions
```

show credit-control statistics

Displays credit control statistics.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show credit-control statistics cc-service *name*

cc-service

Specifies the Credit Control Service name.
name must be an existing Credit Control Service expressed as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to show active credit control statistics.

Example

The following command shows the configured credit control statistics for a service named *service1*:

```
show credit-control statistics cc-service service1
```

show crypto group

Displays information pertaining to configured crypto groups.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show crypto group [name *group_name* **| summary]**

name *group_name*

Displays information for an existing crypto group specified as an alphanumeric string of 1 through 127 characters.

summary

Displays state and statistical information for configured crypto groups in this context.

Usage

Use this command to display information and statistics pertaining to one or all configured crypto groups within the current context.
If the **summary** keyword is not used, detailed information is displayed.
The following command displays detailed information for a crypto group called *group1*:

```
show crypto group name group1
```

show crypto ikev1

Displays pre-shared key information for peer security gateways configured within the context.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show crypto ikev1 { keys | policy [*preference* **] | security-associations [summary] }**

keys

Displays the IKE pre-shared key information based on the peer security gateway.

policy [*preference* **]**

Displays configuration information for the Internet Exchange Key (IKE) policy priority specified as an integer from 1 through 100. If no preference is specified, information will be displayed for all configured policies.

security-associations [summary]

Displays information for established IPSec security associations (SAs).

Usage

Use this command to:

- Display pre-shared key information. This information can be used to verify configuration and/or for troubleshooting.
- Verify the configuration of IKE policies within the context.
- Display established IPSec SA information. This information can be used for troubleshooting.

Example

The following command lists the pre-shared keys received from peer security gateways as part of the Diffie-Hellman exchange:

```
show crypto ikev1 keys
```

The following command displays information for an IKE policy with a preference of *1*:

```
show crypto ikev1 policy 1
```

The following command displays the currently established SAs:

```
show crypto ikev1 security-associations summary
```

show crypto ikev2-ikesa security-associations summary

Displays a summary view of Internet Key Exchange v2 (IKEv2) IKE Security Associations (IKE SAs).

Product

PDIF

Privilege

Administrator, Security Administrator

Syntax

```
show crypto ikev2-ikesa security-associations summary
```

Usage

Shows a summary of the of the SAs configured for a crypto template. It shows the total configured SA lifetime in seconds and the number of seconds left on the timer.

Example

Use this command to create the SA summary:

```
show crypto ikev2-ikesa security-associations summary
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show crypto ikev2-ikesa transform-set

Displays IKEv2/IKESA (Internet Key Exchange v2/IKE Security Association) transform set configuration information.

Product

All using IKEv2/IPSec

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show crypto ikev2-ikesa transform-set *transform_set_name*

show crypto ikev2-ikesa transform-set

Specifies the name of an existing IKEv2/IKSA transform set for which to display information as an alphanumeric string of 1 through 127 characters that is case sensitive.

Usage

Use this command to verify the configuration of IKEv2/IKESA transform sets within the context.
If no keyword is specified, information will be displayed for all IKEv2/IKESA transform sets configured within the context.

Example

The following command displays information for an IKEv2/IKESA transform set named *test1*:

```
show crypto ikev2-ikesa transform-set test1
```

show crypto ipsec

Displays IPSec security associations (SAs) configured within or facilitated by the context and can optionally display statistics for them.

Product

PDSN, GGSN, PDIF, SCM

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show crypto ipsec security-associations map-type { ipsec-3gpp-cscf-subscriber | ipsec-dynamic | ipsec-ikev1 | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip } | summary [distribution | ipsecmgr *ipsec_mgr_id* **| map-type** *map_type* **] | tag** *map_name*

---

map-type { ipsec-dynamic | ipsec-ikev1 | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip }

Specifies that information for all crypto maps of a specific type configured within the context will be displayed. The following types can be specified:

- **ipsec-3gpp-cscf-subscriber**: P-CSCF Subscriber IPSec Tunnel
- **ipsec-dynamic**: Dynamic IPSec Tunnel
- **ipsec-ikev1**: IKEv1 IPSec Tunnel
- **ipsec-ikev2-subscriber**: IKEv2 Subscriber Tunnel
- **ipsec-l2tp**: L2TP IPSec Tunnel
- **ipsec-manual**: Manual (Static) IPSec Tunnel
- **ipsec-mobile-ip**: Mobile IP IPSec Tunnel

---

summary [distribution | ipsecmgr *ipsec_mgr_id* **| map-type** *map_type* **| template-map** *map_name* **]**

Displays only security association summary information.
distribution: Show IPSec Manager SA distribution information.
ipsecmgr *ipsec_mgr_id*: Displays summary SA information for the IPSec manager instance ID specified as an integer from 1 through 200.
map-type *map_type*: Displays summary SA information for the specified type of crypto map.The following types can be specified:

- **ipsec-3gpp-cscf-subscriber**: P-CSCF Subscriber IPSec Tunnel
- **ipsec-dynamic**: Dynamic IPSec Tunnel
- **ipsec-ikev1**: IKEv1 IPSec Tunnel
- **ipsec-l2tp**: L2TP IPSec Tunnel
- **ipsec-manual**: Manual (Static) IPSec Tunnel
- **ipsec-mobile-ip**: Mobile IP IPSec Tunnel

tag *map_name*

Displays the SAs for an existing crypto map specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

Usage

Use this command to display IPSec SA information and statistics. This information can be used for performance monitoring and/or troubleshooting.
The displayed information categorizes control signal and data statistics. Data statistics are further categorized according to the encapsulation method, either GRE or IP-in-IP.

Example

The following command displays summary SA statistics for all IPSec managers.

```
show crypto ipsec security-associations summary
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show crypto ipsec transform-set

Displays IPSec transform set configuration information.

Product

PDG/TTG, PDIF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show crypto ipsec transform-set [*transform_name* **]**

transform_name

Displays information for the IPSec transform set specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

Usage

Use this command to verify the configuration of IPSec transform sets within the context.
If no keyword is specified, information will be displayed for all IPSec transform sets configured within the context.

Important: This command is used in PDIF Release 8.3 only.

Example

The following command displays information for an IPSec transform set named *test1*:

```
show crypto ipsec transform-set test1
```

show crypto isakmp keys

Displays pre-shared key information (Internet Security Association and Key Management Protocol, ISAKMP) for peer security gateways configured within the context.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show crypto isakmp keys
```

Usage

Use this command to display pre-shared key information based on the peer security gateway. This information can be used to verify configuration and/or for troubleshooting.

Example

The following command lists the pre-shared keys received from peer security gateways as part of the Diffie-Hellman exchange:

```
show crypto isakmp keys
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show crypto isakmp policy

Displays Internet Security Association and Key Management Protocol (ISAKMP) policy configuration information.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show crypto isakmp policy [*preference* **]**

preference

Displays configuration information for the ISAKMP policy priority specified as an integer from 1 through 100.

Usage

Use this command to verify the configuration of ISAKMP policies within the context.
If no *preference* is specified, information will be displayed for all configured policies.

Example

The following command displays information for an ISAKMP policy with a preference of *1*:

```
show crypto isakmp policy 1 1
```

show crypto isakmp security-associations

Displays currently established Internet key Exchange (IKE) security associations (SAs) facilitated by the context.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show crypto isakmp security-associations [ cookies ]
```

cookies

Specifies that cookies should be displayed.

Usage

Use this command to display established IPSec SA information. This information can be used for troubleshooting.

Example

The following command displays the currently established SAs:

```
show crypto isakmp security-associations
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show crypto managers

Displays statistics per IPSec Manager.

Product

PDSN, GGSN, PDIF, SCM

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show crypto managers [context *context_name* **| crypto-map** *map_name* **| instance** *instance_num* **| summary [distribution | ike-stats | ipsec-3gpp-cscf-stats | ikev2-stats [demux-stats] | ipsec-sa-stats | npu-stats]]**

context *context_id*

Displays IPSec manager statistics for an existing context specified as n alphanumeric string of 1 through 80 characters.

crypto-map *map_name*

Displays IPSec Managers for an existing crypto map specified as an alphanumeric string of 1 through 128 characters.

instance *instance_num*

Displays statistics for the IPSec manager instance specified as an integer from 1 through 366.

summary [distribution | ike-stats | ipsec-3gpp-cscf-stats | ikev2-stats [demux-stats] | ipsec-sa-stats | npu-stats]

Shows statistics per service IP address for each manager.
distribution: Displays a summary list of IPSec manager distribution.
ike-stats: Displays a summary list of IPSec IKE statistics. for each IPSec manager.
ipsec-3gpp-cscf-stats: Displays CSCF IPSec Statistics on each IPSec Manager.
ikev2-stats: Displays IKEv2 Statistics on each IPSec Manager.
- **demux-stats**: Displays session demux statistics on each IPSec Manager.

ipsec-sa-stats: Displays a summary list of IPSec Security Association (SA) statistics for each IPSec Manager.
npu-stats: Displays NPU statistics on each IPSec Manager.

Usage

Use this command to view statistics relating to IPSec managers.

Example

The following command displays summary information for all IPSec managers:

```
show crypto managers summary
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show crypto map

Displays crypto map configuration information.

Product

PDIF, PDSN, GGSN, SCM

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show crypto map [map-type [ipsec-3gpp-cscf-subscriber | ipsec-dynamic | ipsec-ikev1 | ipsec-ikev2-subscriber | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip] | tag *map_name* **| summary]**

map-type [ipsec-3gpp-cscf-subscriber | ipsec-dynamic | ipsec-ikev1 | ipsec-ikev2-subscriber | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip]

Specifies that information for all crypto maps of a specific type configured within the context will be displayed. The following types can be specified:

- **ipsec-3gpp-cscf-subscriber**: P-CSCF subscriber IPSec Tunnel
- **ipsec-dynamic**: Dynamic IPSec Tunnel
- **ipsec-ikev1**: IKEv1 IPSec Tunnel
- **ipsec-ikev2-subscriber**: IKEv2 Subscriber Tunnel
- **ipsec-l2tp**: L2TP IPSec Tunnel
- **ipsec-manual**: Manual (Static) IPSec Tunnel
- **ipsec-mobile-ip**: Mobile IP IPSec Tunnel

tag *map_name*

Specifies the name of an existing crypto map in the current context for which to display configuration information as an alphanumeric string of 1 through 127 characters that is case sensitive.

summary

Displays summary information for all crypto maps configured in the context.

Usage

Use this command to verify the configuration of crypto maps within the context.
If no keyword is specified, information will be displayed for all maps configured within the context regardless of type.

Example

The following command displays configuration information for a dynamic crypto map named *test_map3*:

```
show crypto map tag test_map3
```

show crypto statistics

Displays Internet Protocol Security (IPSec) statistics.

Product

PDSN, GGSN, PDG/TTG, PDIF, SCM

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show crypto statistics ikev1 | ikev2 [service-ip-address *ip-address* **] [service-name** *name* **] | ipsec-3gpp-cscf [service-ip-address** *ip-address* **] [service-name** *name* **]| srtp [service-ip-address** *ip-address* **] [service-name** *name* **]**

ikev1

Displays global ikev1 statistics for this context.

ikev2 [service-ip-address *ip-address* **] [service-name** *name* **]**

Displays global ikev2 statistics for this context.
service-ip-address *ip-address*: Specifies the Packet Data Interworking Function (PDIF) service IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.
service-name *name*: Specified PDIF service name.

ipsec-3gpp-cscf [service-ip-address *ip-address* **] [service-name** *name* **]**

Displays global CSCF IPSec SA statistics for this context.
service-ip-address *ip-address*: Specifies the CSCF service IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.
service-name *name*: Specifies the CSCF service name.

srtp [service-ip-address *ip-address* **] [service-name** *name* **]**

Displays global SRTP (Secure Real-time Transport Protocol) statistics for this context.
service-ip-address *ip-address*: Specifies the CSCF service IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.
service-name *name*: Specifies the CSCF service name.

Usage

Use this command to display statistics for IPSec tunnels facilitated by the context. This information can be used for performance monitoring and/or troubleshooting

Example

The following command displays cumulative IPSec statistics for the current context:

```
show crypto statistics
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show crypto transform-set

Displays transform set configuration information.

Product

PDIF, PDSN, GGSN, SCM

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show crypto transform-set [*transform_name* **]**

transform_name

Specifies the name of an existing transform set for which to display information as an alphanumeric string of 1 through 127 characters that is case sensitive.

Usage

Use this command to verify the configuration of transform sets within the context.
If no keyword is specified, information will be displayed for all transform sets configured within the context.

Important: This command is used in PDIF Release 8.1. In PDIF Release 8.3, the syntax of this command is changed to **show crypto ipsec transform-set**.

Example

The following command displays information for a transform set named *test1*:

```
show crypto transform-set test1
```

show cs-network

Displays statistics for the Circuit Switched (CS)-network(s) instance configured on a chassis for HNB-GW service sessions.

Product

HNB-GW

Privilege

Security Administrator, Administrator, Operator

Syntax

show cs-network { all | name *cs_name* **} [status] [| { grep** *grep_options* **| more }]**

all

Displays status counters for all CS (circuit switched) networks configured for HNB-GW service sessions on a chassis.

name *cs_name*

Displays status counters for a CS network configured for HNB-GW service specified as an alphanumeric string of 1 through 127 characters that is case sensitive

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage

Use this command to display the status of any or all CS-network(s) instance configured on a chassis for HNB-GW service sessions.

Example

The following command displays the output for CS network instance status named *cs_1_hnb*:

```
show cs-network name cs_1_hnb status
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cs-network counters

Displays the session counter information for an HNB-CS Network associated with Home-NodeB Gateway (HNB-GW) services configured and running on a system.

Product

HNB-GW

Privilege

Inspector

Syntax

show cs-network counters [name *cs_svc_name* **[msc** *msc_point_code* **]] [| { grep** *grep_options* **| more }]**

name *cs_svc_name*

Filters the counter display based on an existing HNB-CS Network service name associated with an HNB-GW service running on system. *cs_svc_name* is an alphanumeric string of 1 through 63 characters.

msc *msc_point_code*

Filters the counter display filtered on the basis of MSC address provided in the SS7 point code that is connected to a particular HNB-CS Network service. *msc_point_code* must be the address of an MSC in SS7 point code notation.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter.

Usage

Use this command to view the session counter information for HNB-CS Network services configured and MSCs connected on a system.

Example

The following command displays the counters for the HNB-CS Network service named *hnb_cs_svc1*:

```
show cs-network counters name hnb_cs_svc1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cs-network statistics

Displays the Circuit Switched session statistics for Home-NodeB Gateway (HNB-GW) services configured and running on this system.

Product

HNB-GW

Privilege

Inspector

Syntax

show cs-network statistics [name *cs_svc_name* **| ranap-only | rtp-only | sccp-only] [| { grep** *grep_options* **| more }]**

name *cs_svc_name*

Filters the session statistics display based on an existing HNB-CS Network service name that is associated with an HNB-GW service running on this system. *cs_svc_name* is an alphanumeric string of 1 through 63 characters.

ranap-only

Filters the session statistics to display only Radio Access Network Application Protocol (RANAP) traffic for an HNB-CS Network service which is configured and associated with an HNB-GW service running on this system.

rtp-only

Filters the session statistics to display only Realtime Streaming Protocol (RTP) and Realtime Streaming Control Protocol (RTCP) traffic for the specified HNB-CS Network service which is configured and associated with an HNB-GW service running on this system.

sccp-only

Filters the session statistics to display only Signaling Connection Control Part (SCCP) traffic for the specified HNB-CS Network service which is configured and associated with an HNB-GW service running on this system.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter of the *Command Line Interface Reference*.

Usage

Use this command to view the session statistics for overall session or in selected part of user session for HNB-GW services configured and running on this system.

Example

The following command displays the session statistics for RTP and RTCP part of session for the HNB-CS Network service named *hnb_cs1*:

```
show cs-network statistics name hnbcs1 rtp-only
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cscf ifc

Displays the Initial Filter Criteria (iFC) for shared iFC functionality.

Product

SCM (S-CSCF, SIP Proxy)

Privilege

Security Administrator, Administrator

Syntax

show cscf ifc { all | id *fc_id* **} [| { grep** *grep_options* **| more }]**

all | id *fc_id*

all: Displays all iFC.
id *fc_id*: Displays information for an existing iFC specified as an alphanumeric string of 1 through 200 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage

Use this command to display configuration information for any or all iFC on this system.

Example

The following command displays the configuration information for all iFC on this system:

```
show cscf ifc all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cscf nat

Displays the Call Session Control Function (CSCF) mapping created for each of the media streams present in an established dialog.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Syntax

show cscf nat media mapping { all | aor *aor* **} [| { grep** *grep_options* **| more }]**

media mapping { all | aor *aor* **}**

all: Displays the UE/Network origins and destinations, including their IP addresses/port numbers and associated contexts.
aor *aor*: Displays information for an Address of Record (AoR) specified as an alphanumeric string of 1 through 79 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage

Use this command to display the status of configured Network Address Translation (NAT) support.

Example

The following command displays the status of the mapping created for each of the media streams present on this system:

```
show cscf nat media mapping all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cscf npdb-servers

Displays the connection status of NPDB (Number Portability Data Base) servers in S-CSCF service.

Product

SCM (S-CSCF)

Privilege

Security Administrator, Administrator

Syntax

show cscf npdb-servers service *service_name* **[| { grep** *grep_options* **| more }]**

service *service_name*

Specifies the name of an existing CSCF service for which the statistics will be displayed as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage

Use this command to display the connection status of NPDB servers in S-CSCF service.

Example

The following command displays the connection status of NPDB servers for the S-CSCF service named *scscf1*:

```
show cscf npdb-servers service scscf1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cscf peer-servers

Displays name, IP address, and status of configured Call Session Control Function (CSCF) peer servers visible to the system.

Product

SCM

Privilege

Security Administrator, Administrator, Operator

Syntax

show cscf peer-servers { all | full | name *service_name* **[server-name** *server_name* **] } [| { grep** *grep_options* **| more }]**

all | full | name *service_name* **[server-name** *server_name* **]**

all: Displays the peer server list names and the servers within those lists including their IP addresses/port numbers and domain names.
full: Displays additional details regarding the peer servers within the configured lists on the system.
name *service_name* **[server-name** *server_name* **]**: Displays the same information as the full keyword output, but for a peer server list or an existing peer server specified as an alphanumeric string of 1 through 80 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage

Use this command to display the status of configured peer servers.

Example

The following command displays the status of a peer server named *icscf3* that is a member of peer server list *cscf-main*:

```
show cscf peer-servers name cscf-main server-name icscf3
```

The following command displays the status of all peer servers in configured peer server groups in this context:

```
show cscf peer-servers full
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cscf service

Displays configuration and/or statistical information for Call Session Control Function (CSCF) services on this system.

Product

SCM

Privilege

Security Administrator, Administrator, Operator

Syntax

show cscf service { all [counters] | diameter { location-info statistics service-name *service_name* **[vpn-name** *name* **] | policy-control statistics service-name** *service_name* **[vpn-name** *name* **] } | grey-list name** *name* **| li-packet-cable statistics service-name** *service_name* **| performance-counters name** *service_name* **| statistics name** *service_name* **[all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp { msrp | sip }] | subscription name** *service_name* **} [| { grep** *grep_options* **| more }]**

---

all [counters]

Displays configuration information for all CSCF services configured on this system.
counters: Displays statistics with the configuration information for all CSCF services configured on the system.

---

diameter { location-info statistics service-name *service_name* **[vpn-name** *name* **] | policy-control statistics service-name** *service_name* **[vpn-name** *name* **] }**

location-info statistics: Displays Diameter statistics on the E2 interface with the location information.
policy-control statistics: Displays Diameter (DPECA) statistics on the CSCF Rx interface with the configuration information.
service-name *service_name*: Specifies the name of an existing CSCF service for which the statistics will be displayed as an alphanumeric string of 1 through 63 characters.
vpn-name *name*: Specifies the name of an existing context in which all statistics for all services will be displayed as an alphanumeric string of 1 through 79 characters.

---

grey-list name *name*

Displays an existing list of run-time grey-listed users and their remaining barred period for the specified CSCF service as an alphanumeric string of 1 through 63 characters.

---

li-packet-cable statistics service-name *service_name*

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

---

name *service_name* **[counters]**

Displays configuration information for an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.
counters: Displays statistics with the configuration information for the specific CSCF service.

performance-counters name *service_name*

Displays performance counters (3GPP TS 32.409) for an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.

statistics name *service_name* **[all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp { msrp | sip }]**

Displays service statistics for an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.
all: Displays all CSCF service statistics.
calls: Displays session statistics related to CSCF calls.
ip-security: Displays session statistics related to CSCF IPSec.
message: Displays session statistics for the SIP method MESSAGE.
package-name: Displays session statistics for the associated event package.

- **message-summary**: Displays session statistics for the "message-summary" event package.
- **presence**: Displays session statistics for the "presence" event package.
- **reg**: Displays session statistics for the "reg" event package.
- **winfo**: Displays session statistics for the "watcher-info" event package.

registrations: Displays session statistics related to CSCF registrations, re-registrations, and de-registrations.
sigcomp: Displays session statistics related to CSCF sigcomp.
tcp: Displays session statistics related to CSCF TCP.

- **msrp**: Displays statistics related to CSCF TCP MSRP statistics.
- **sip**: Displays statistics related to CSCF TCP SIP statistics.

Important: This keyword must be followed by another statistics-related keyword.

subscription name *service_name*

Displays service level subscription information for an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display configuration information and/or statistics for any or all CSCF services on this system.

Example

The following command displays service statistics for the CSCF service named *cscf1*:

```
show cscf service statistics name cscf1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cscf sessions

Displays statistics for Call Session Control Function (CSCF) sessions on this system.

Product

SCM

Privilege

Security Administrator, Administrator, Operator

Syntax

show cscf sessions { counters { calls { duration | first-response-time | invite-processing-time | post-answer-delay | post-dial-delay | service *service_name* **| session-release-delay | session-setup-delay } service** *service_name* **| subscription { duration | service** *service_name* **| setup-time } service** *service_name* **} | duration | full [callleg-id** *id* **| from-aor** *aor* **| service** *service_name* **| session-id** *id* **| to-aor** *aor* **] [media-type** *type* **] | summary [from-aor** *aor* **| service** *service_name* **| session-id** *id* **| to-aor** *aor* **] } [| { grep** *grep_options* **| more }]**

counters { calls { duration | first-response-time | invite-processing-time | post-answer-delay | post-dial-delay | service *service_name* **| session-release-delay | session-setup-delay } service** *service_name* **| subscription { duration | service** *service_name* **| setup-time } service** *service_name* **}**

Displays counters for all CSCF sessions matching the filter criteria.
calls: Counters associated with calls in CSCF service.

- **duration**: Displays the call duration time.
- **first-response-time**: Displays the time interval for the first response received for INVITE.
- **invite-processing-time**: Displays the INVITE message processing time in CSCF.
- **post-answer-delay**: Displays the time interval for post answer delay.
- **post-dial-delay**: Displays the time interval for the ringing or success response for INVITE.
- **service** *service_name*: Displays counters for an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.

  Important: This keyword may be used alone with the **counters** keyword or following any other counters-specific keyword.

- **session-release-delay**: Displays the time interval for releasing the call.
- **session-setup-delay**: Displays the time interval for session setup.
- **subscription**: Counters associated with subscriptions in CSCF service.
  - **duration**: Displays the SIP Subscription duration time.
  - **service** *service_name*: Displays specific service. *service_name* must be an existing CSCF service and be from 1 to 63 alphanumeric characters.

    Important: This keyword may be used alone with the **subscription** keyword or following any other subscription-specific keyword.

- **setup-time**: Displays the SIP Subscription setup time.

duration

Displays the call duration for all CSCF sessions.

full [callleg-id *id* **| from-aor** *aor* **| service** *service_name* **| session-id** *id* **| to-aor** *aor* **] [media-type** *type* **]**

Displays all the session information for the active CSCF sessions matching the filter criteria.
callleg-id *id*: Displays session statistics for an existing call-leg ID expressed as an alphanumeric string of 1 through 63 characters.
from-aor *aor*: Displays session statistics for sessions originating from an existing Address of Record (AoR) specified as an alphanumeric string of 1 through 79 characters.
service *service_name*: Displays session statistics for sessions using an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.
session-id *id*: Displays session statistics for sessions with an existing ID specified as an alphanumeric string of 1 through 63 characters.
to-aor *aor*: Displays session statistics for sessions sent to an existing AoR specified as an alphanumeric string of 1 through 79 characters.
media-type *type*: Displays information about an existing media type specified as an alphanumeric string of 1 through 9 characters.

summary [from-aor *aor* **| service** *service_name* **| session-id** *id* **| to-aor** *aor* **]**

Displays session summary information for sessions matching the filter criteria.
from-aor *aor*: Displays session statistics for sessions originating from an existing AoR specified as an alphanumeric string of 1 through 79 characters.
service *service_name*: Displays session statistics for sessions using an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.
session-id *id*: Displays session statistics for sessions with an existing ID specified as an alphanumeric string of 1 through 63 characters.
to-aor *aor*: Displays session statistics for sessions sent to an existing AoR specified as an alphanumeric string of 1 through 79 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage

Use this command to display session information for any or all CSCF sessions.

Example

The following command displays the output for CSCF session duration:

```
show cscf sessions duration
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cscf sip

Displays Session Initiation Protocol (SIP) statistics for a specific Call Session Control Function (CSCF) service configured on this system.

Product

SCM

Privilege

Security Administrator, Administrator, Operator

Syntax

show cscf sip statistics name *service_name* **[interface { domain { list | name** *domain_name* **} | ip { address** *ip_address* **| list } } | vpn-name** *name* **] [| { grep** *grep_options* **| more }]**

statistics name *service_name*

Specifies the name of an existing CSCF service as an alphanumeric string of 1 through 63 characters.

[interface { domain { list | name *domain_name* **} | ip { address** *ip_address* **| list } }**

SIP statistics will be displayed for this interface.
domain list: Displays list of interfaces associated with the CSCF service.
domain name *domain_name*: Specifies an existing domain associated with the CSCF service as an alphanumeric string of 1 through 80 characters.
ip address *ip_address*: Specifies the destination or source IP address associated with the CSCF service in IPv4 dotted-decimal or IPv6 colon-separated notation.
ip list: Displays a list of interfaces associated with the CSCF service.

vpn-name *name*

Specifies the name of an existing VPN as an alphanumeric string of 1 through 79 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage

Use this command to display SIP statistics for a specific CSCF service.

Important: This command displays counters for SIP statistics for a specified CSCF service. Counters are incriminated when SIP messages are sent (Tx) or received (Rx). SIP Request, Response, and Error counters are maintained at various levels in the SIP stack. These values are dependent on the packet flow. For example, if packets are dropped at an initial stage of parsing and error detection, the counters may not increment. All 2xx Response counters for individual requests are maintain outside the SIP layer and will not track re-transmissions and erroneous packets that are dropped. All other counters do keep track of re-transmissions.

Example

The following command displays SIP statistics for the CSCF service named *cscf1*:

```
show cscf sip statistics name cscf1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show cscf tcp

Displays TCP connection information for a specific Call Session Control Function (CSCF) service configured on this system.

Product

SCM

Privilege

Security Administrator, Administrator, Operator

Syntax

show cscf tcp connections service *service_name* **[facility { cscfmgr | sessmgr }] [full] [msrp] [remote-ip** *ip_address* **] [remote-port** *port_number* **] [sip] [| { grep** *grep_options* **| more }]**

---

connections service *service_name*

Specifies the name of an existing CSCF service as an alphanumeric string of 1 through 63 characters.

---

facility { cscfmgr | sessmgr }

Facility type for which connection details have to be retrieved.
cscfmgr: Facility type cscfmgr.
sessmgr: Facility type sessmgr.

---

full

Displays detailed information related to each connection.

---

msrp

Displays statistics related to CSCF TCP Message Session Relay Protocol (MSRP) statistics.

---

remote-ip *ip_address*

Specifies the remote IP address to match the connection in IPv4 dotted-decimal or IPv6 colon-separated notation.

---

remote-port *port_number*

Specifies the remote port to match the connection an integer from 1 through 65534.

---

sip

Displays statistics related to CSCF TCP SIP statistics.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage

Use this command to display TCP connection information for a specific CSCF service.

Important: More than one optional keyword may be used per command.

Example

The following command displays TCP connections for the CSCF service named *cscf1*:

```
show cscf tcp connections service cscf1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show css delivery-sequence

In StarOS 9.0 and later releases, this command is obsolete.

show css server

In StarOS 9.0 and later releases, this command is obsolete.

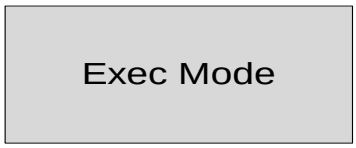
show css service

In StarOS 9.0 and later releases, this command is obsolete.

Chapter 115
Exec Mode Show Commands (D-G)

This section includes the commands **`show dhcp`** through **`show gtpu-service`**.

The Exec Mode is the initial entry point into the command line interface system. Exec mode **show** commands are useful in troubleshooting and basic system monitoring.



show dhcp

Displays counter information pertaining to Dynamic Host Configuration Protocol (DHCP) functionality based on specific criteria.

Product

GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show dhcp [**counters** | **full** | **summary**] [**all** | **apn** *apn_name* | **callid** *id* | **chaddr** *mac_address* | **dhcp-service** *svc_name* | **imsi** *imsi* | **user-address** *address* | **msid** *msid* | **server** *server_address* | **username** *name*]

counters

Displays DHCP counter information.

full

Displays all available information pertaining to the criteria specified.

summary

Displays a summary of the DHCP statistics.

all

Displays counter information for each active PDP context.

apn *apn_name*

Displays information based on an existing Access Point Name (APN) specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

callid *id*

Displays information for an existing call identification number specified as a 4-digit hexadecimal number.

chaddr *mac_address*

Displays information for a mobile node specified by its MAC address.

dhcp-service *svc_name*

Displays information for an existing DHCP service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

imsi *imsi*

Displays information for an International Mobile Subscriber Identity (IMSI) specified as a string of 1 to 15 digits.

user-address *address*

Displays information for a DHCP-assigned user IP address specified in IPv4 dotted-decimal notation.

msid *msid*

Displays information for a Mobile Subscriber Identity (MSID) specified as a string of 1 to 15 digits.

server *server_address*

Displays information for a DHCP server specified by its IP address in IPv4 dotted-decimal notation.

username *name*

Displays information for a subscriber specified as an alphanumeric string of 1 through 127 characters (including wildcards "$" and "*") that is case sensitive.

Usage

Counters pertaining to DHCP functionality can be displayed as cumulative values or for specific APNs, PDP contexts, servers, or DHCP services.

Example

The following command displays DHCP counter information for a DHCP service called *DHCP-Gi*:

```
show dhcp dhcp-service DHCP-Gi
```

The following command displays DHCP counter information for a DHCP Call ID *01ca11a2*:

```
show dhcp call-id DHCP-Gi
```

The following command displays DHCP information for the specified mobile node:

```
show dhcp chaddr 00:05:47:00:37:44
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show dhcp statistics

Displays Dynamic Host Configuration Protocol (DHCP) statistics for the specified servers.

Product

GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show dhcp statistics [dhcp-service *svc_name* **| server** *ip_address* **]**

dhcp-service *svc_name*

Displays statistics for a DHCP service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

server *ip_address*

Displays statistics for a DHCP server specified by its IP address in IPv4 dotted-decimal notation.

Usage

Statistics for a single DHCP service or DHCP server can be viewed using the **dhcp-service** or **server** keywords respectively.
Cumulative statistics for all DHCP services and servers within a context can be viewed by executing the command with no keywords from within the context in which they're configured.
If this command is issued from within the local context, the statistics displayed will be cumulative for all dhcp servers configured on the system regardless of context.

Example

The following command allows you to view statistics for all configured DHCP servers within the context:

```
show dhcp statistics
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show dhcp-service

Displays configuration information for either a specific, or for all Dynamic Host Configuration Protocol (DHCP) servers configured.

Product

GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show dhcp-service { all | name svc_name }
```

all

Displays information for all configured DHCP services.

name *svc_name*

Displays information for a DHCP service name specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage

This command is used to verify the configuration of one or all DHCP services for monitoring or troubleshooting purposes. The output is a concise listing of DHCP service parameter settings.
If this command is executed from within the local context with the all keyword, information for all DHCP services configured on the system will be displayed.

Example

The following command displays configuration information for a DHCP service called *dhcp1*:

```
show dhcp-service name dhcp1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show dhcp status

Displays configuration information for either a specific, or for all Dynamic Host Configuration Protocol (DHCP) services and servers configured.

Product

GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show dhcp status [dhcp-service *svc_name* **] [server** *ip_addr* **]**

all

Displays information for all configured DHCP services.

dhcp-service *svc_name*

Displays information for a DHCP service name specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

server *ip_address*

Displays status for a DHCP server specified by its IP address in IPv4 dotted-decimal notation.

Usage

This command is used to show/verify the status or configuration of one or all DHCP services along with count of cumulative leased addresses and addresses leased at that time for monitoring or troubleshooting purposes. The output is a concise listing of DHCP service parameter settings.
If this command is executed from within the local context with the all keyword, information for all DHCP services configured on the system will be displayed.

Example

The following command displays status of a DHCP service called *ggsn_dhcp1*:

```
show dhcp status dhcp-service ggsn_dhcp1
```

State shown in display is consolidated across session managers, such as for each session manager, DHCP server have a timestamp value associated with its state.
For a DHCP server, its timestamp value is compared for each session manager and the state associated with the latest value is shown.

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show diameter aaa-statistics

Displays Diameter Authentication, Authorization and Accounting (AAA) statistics.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show diameter aaa-statistics [all | group *group_name* **[server** *server_name* **] | server** *server_name* **] [| { grep** *grep_options* **| more }]**

all

Displays all available Diameter server statistics.

group *group_name* **[server** *server_name* **]**

Displays all Diameter server statistics within an existing AAA group specified as an alphanumeric string of 1 through 64 characters.
server_name must be the name of a Diameter server, expressed as an alphanumeric string of 1 through 64 characters.

server *server_name*

Displays Diameter server statistics for the Diameter server name specified as an alphanumeric string of 1 through 64 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to view Diameter AAA statistics.

Example

The following command displays all available Diameter server statistics:

```
show diameter aaa-statistics all
```

show diameter accounting servers aaa-group

Displays Diameter accounting server information for an Authentication, Authorization and Accounting (AAA) group.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show diameter accounting servers [aaa-group *group_name* **] [| { grep** *grep_options* **| more }]**

aaa-group *group_name*

Specifies the name of an existing AAA group as an alphanumeric string of 0 through 64 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to view Diameter accounting server information for an AAA group.

Example

The following command displays Diameter accounting server information for an AAA group named in *group12*:

```
show diameter accounting servers aaa-group group12
```

show diameter authentication servers aaa-group

Displays Diameter Authentication server information for a specified AAA group.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show diameter authentication servers [aaa-group *group_name* **]**

aaa-group *group_name*

Specifies the name of an existing AAA group as an alphanumeric string of 0 through 64 characters.

Usage

Use this command to view Diameter authentication server information for an AAA group.

Example

The following command displays Diameter authentication server information for an AAA group named *group12*:

```
show diameter authentication servers aaa-group group12
```

show diameter endpoint

This command has been deprecated, and is replaced by the show diameter endpoints command.

show diameter endpoints

This command displays the status of Diameter client endpoint(s).

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show diameter endpoints { all | endpoint *endpoint_name* **} [| { grep** *grep_options* **| more }]**

all

Displays status of all Diameter client endpoints.

endpoint *endpoint_name*

Displays status of an existing Diameter client endpoint specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to view the status of Diameter client endpoints.
If you are in the local context, then all contexts are searched for the specified endpoint(s). Specify **all** to see all endpoints; otherwise, just the named endpoint will be displayed. If no argument is provided, a summary of all endpoints is displayed.
Default value: N/A

Example

The following command displays status of all Diameter client endpoints.

```
show diameter endpoints all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show diameter message-queue

Displays Diameter message queue statistics.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show diameter message-queue counters { inbound | outbound } [endpoint *endpoint_name* **[peer-host** *peer_id* **[peer-realm** *realm_id* **]] | session-id** *session_id* **] [| { grep** *grep_options* **| more }]**

counters { inbound | outbound }

Specifies the message counters:
inbound: Specifies Diameter inbound messages
outbound: Specifies Diameter outbound messages

endpoint *endpoint_name*

Specifies the Diameter endpoint as an alphanumeric string of 1 through 63 characters.

peer-host *peer_id*

Specifies the Diameter peer host as an alphanumeric string of 1 through 63 characters.

peer-realm *realm_id*

Specifies the Diameter peer realm as an alphanumeric string of 1 through 127 characters.

session-id *session_id*

Specifies the session ID as an alphanumeric string of 1 through 127 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to view the count of the messages in the Diameter message queue for specific counter type, session ID, or endpoint, peer host, and peer realm.

Example

The following command displays message queue statistics for outbound messages specific to the Diameter endpoint named *asr5k.testnetwork.com*:

```
show diameter message-queue counters outbound endpoint
asr5k.testnetwork.com
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show diameter peers

Displays Diameter peer information.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show diameter peers [full | summary] [all | [endpoint *endpoint_name* **] [peer-host** *peer_id* **] [peer-realm** *realm_id* **]+] [| { grep** *grep_options* **| more }]**

full

Displays full details of all or specified Diameter peers.

summary

Displays summary details of all or specified Diameter peer(s).

all

Displays details of all Diameter peers.

endpoint *endpoint_name*

Displays details of the origin Diameter endpoint specified as an alphanumeric string of 1 through 255 characters.

peer-host *peer_id*

Displays details of the Diameter peer host specified as an alphanumeric string of 1 through to 63 characters.

peer-realm *realm_id*

Displays details of the Diameter peer realm ID specified as an alphanumeric string of 1 through 127 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to view the details of Diameter peers.
If you are in the local context, then all contexts are searched for the specified peer(s).
This is similar to the **show subscribers** CLI command and supports multiple filter options specified at the same time.

If filter options are specified (e.g., **all**, **endpoint**, etc.), the default is for one line of output to be displayed per peer. Use **full** to get detailed information per peer, or **summary** to get summarized information about all matching peers.
If no filter options are specified, a summary output for all peers is displayed. Use the **full** option to get detailed information about every peer.
Default value: N/A

Example

The following command details of the Diameter endpoint named *endpoint12*:

```
show diameter peers endpoint wndpoint12
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show diameter route status

Displays Diameter route health status information.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show diameter route status [ endpoint endpoint_name | full [ endpoint endpoint_name ] ] [
host host_name | peer peer_id ] [ | { grep grep_options | more } ]
```

full

Displays information about which Diameter clients are using which peer/host combinations.

endpoint *endpoint_name*

Displays detailed information for the Diameter client endpoint specified as an alphanumeric string of 1 through 63 characters.

host *host_name*

Displays information for the Diameter host specified as an alphanumeric string of 1 through 63 characters.

peer *peer_id*

Displays information for the Diameter peer host specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to view the Diameter route health status.
The route status displays status of peer/host combinations. Refer to the **route-failure** CLI command in Diameter Endpoint Configuration mode. When no options are specified, the display will give one line per peer/host combination, indicating how many Diameter clients are using each combination, and for how many clients the combination is available or failed. Specify **full** to see which Diameter clients are using which peer/host combinations. Specify **host** or **peer** to see just combinations with the named host or peer. Specify **endpoint** to see detailed information about the named Diameter client.
Default value: N/A

Example

The following command displays route health status details of the Diameter client endpoint named *endpoint12*:

```
show diameter route status endpoint endpoint12
```

show diameter route table

Displays the Diameter routing table.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show diameter route table [ wide ] [ endpoint endpoint_name ] [ | { grep grep_options | more } ]
```

wide

Displays the route table information in wide-format.

endpoint *endpoint_name*

Displays the Diameter routing table for the Diameter endpoint specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view the status of Diameter client endpoints.
If you are in the local context, then the route information used by Diameter endpoints in all chassis contexts will be used in the display.
The route table displays all static and dynamic routes. Refer to the route-entry CLI command in Diameter Endpoint Configuration Mode.
Default value: N/A

Example

The following command displays status of the Diameter client endpoint named *endpoint12*.

```
show diameter route table endpoint endpoint12
```

show diameter statistics

Displays Diameter peer statistics.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show diameter statistics [[proxy] endpoint *endpoint_name* **[peer-host** *peer_id* **[peer-realm** *realm_id* **]]] [| { grep** *grep_options* **| more }]**

endpoint *endpoint_name*

Displays statistics for the DIameter endpoint specified as an alphanumeric string of 1 through 63 characters.

peer-host *peer_id*

Displays statistics for the Diameter host peer specified as an alphanumeric string of 1 through 255 characters.

peer-realm *realm_id*

Displays statistics for the Diameter peer realm specified as an alphanumeric string of 1 through 127 characters.

proxy

Displays proxy related statistics.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to view Diameter statistics for the specified endpoint or proxy.

Example

The following command displays Diameter peer statistics for the endpoint named *endpoint12*:

```
show diameter statistics endpoint endpoint12
```

show diameter-service

Displays information about configured Diameter services.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show diameter-service { all | lte-s6a trace-id { all | user-name *user_name* **} | name** *service_name* **| statistics name** *service_name* **[vpn-name** *vpn_context_name* **] } [| { grep** *grep_options* **| more }]**

all

Displays full information for all configured Diameter services.

lte-s6a trace-id { all | user-name *user_name* **}**

Displays user trace ID information for an LTE/S6a application.
all: Displays full information.
user-name *user_name*: Displays information for the user specified an alphanumeric string of 1 through 79 characters.

name *service_name*

Displays information for the Diameter service name specified as an alphanumeric string of 1 through 79 characters.

statistics name *service_name* **[vpn-name** *vpn_context_name* **]**

Displays statistics for the Diameter service name specified as an alphanumeric string of 1 through 79 characters.
vpn-name *vpn_context_name*: Specifies the name of VPN context as an alphanumeric string of 1 through 79 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to view information on configured Diameter services.

Example

The following command displays statistics for the Diameter service named *ggsn12*:

```
show diameter-service name ggsn2
```

show dns-client

Displays cache and/or statistics for a specified Domain Name System (DNS) client.

Product

P-CSCF, SIP Proxy, SGSN, HSGW, MME

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show dns-client { cache client *name* **[query-name** *name* **\| query-type { A \| AAAA \| NAPTR \| SRV }] \| statistics client** *name* **} [\| { grep** *grep_options* **\| more }]**

---

cache client *name* **[query-name** *name* **\| query-type { A \| AAAA \| NAPTR \| SRV }]**

displays statistics for the cache of an existing DNS client specified as an alphanumeric string of 1 through 255 characters.
query-name *name*: Filters DNS results based on the domain name specified as an alphanumeric string of 1 through 255 characters. *name* is the domain name used to perform the DNS query. It is different from the actual domain name which is resolved. For example, to resolve the SIP server for *service.com*, the query name is *_sip._udp.service.com* and the query type is **SRV**.
query-type:

- **A**: Filters DNS results based on 32-bit domain IPv4 address records (A records).
- **AAAA**: Filters DNS results based on 128-bit domain IPv6 address records (AAAA resource records).
- **NAPTR**: Filters DNS results based on Naming Authority Pointer records.
- **SRV**: Filters DNS results based on service locator records (SRV records).

---

statistics client *name*

Displays statistics for an existing DNS client specified as an alphanumeric string of 1 through 255 characters.

\| { grep *grep_options* **\| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display DNS cache and/or statistics for a specified DNS client.

Example

The following command displays statistics for a DNS client named *domain1.com*:

```
show dns-client statistics client domain1.com
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show dynamic-policy statistics

Displays policy control and charging (PCC) statistics from the interface communicating with the Policy and Charging Rules Function (PCRF) via Gx(x).

Product

HSGW, PDSN, S-GW

Privilege

Inspector

Syntax

show dynamic-policy statistics { hsgw-service *name* **| pdsn-service** *name* **| sgw-service** *name* **}**

hsgw-service *name*

Displays policy control and charging statistics from the Gxa interface communicating with the PCRF. *name* must be an existing HSGW service name and be from 1 to 63 alphanumeric characters.

pdsn-service *name*

Displays policy control and charging statistics from the Gx interface communicating with the PCRF. *name* must be an existing PDSN service name and be from 1 to 63 alphanumeric characters.

sgw-service *name*

Displays policy control and charging statistics from the Gxc interface communicating with the PCRF. *name* must be an existing S-GW service name and be from 1 to 63 alphanumeric characters.

Usage

Use this command to display PCC statistics for the specified service and its Gx interface communicating with the PCRF.

Example

The following command displays HSGW statistics for an HSGW service named *hsgw4*:

```
show dynamic-policy statistics hsgw-service hsgw4
```

The following command displays PCC statistics for a PDSN service named *cdma4*:

```
show dynamic-policy statistics pdsn-service cdma4
```

The following command displays S-GW statistics for an S-GW service named *sgw4*:

```
show dynamic-policy statistics sgw-service sgw4
```

show egtpc peers

Displays information about eGTP-C peers.

Product

P-GW, S-GW

Privilege

Inspector

Syntax

show egtpc peers [address *ip_address* **| egtp-service** *name* **] | interface { mme | pgw-ingress | sgsn | sgw-egress | sgw-ingress } [address** *ip_address* **] [wf1] }] [| { grep** *grep_options* **| more }]**

---

address *ip_address*

Displays information about a eGTP-C peer specified by its IP address in IPv4 dotted-decimal notation or IPv6 colon-separated notation.

---

egtp-service *name* **[address** *ip_address* **]**

Displays information about eGTP-C peers associated with an existing egtp-service name specified as an alphanumeric string of 1 through 63 characters.
address *ip_address*: Additionally, the results can be filtered based on the IP address associated with an existing eGTP-C peer service specified in IPv4 dotted-decimal notation or IPv6 colon-separated notation.

---

interface { mme | pgw-ingress| sgsn | sgw-egress | sgw-ingress } [address *ip_address* **] [wf1]**

Displays information about eGTP-C peers associated with the service interface configured on this system.
mme: Displays information about eGTP-C MME peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the MME peer.
pgw-ingress: Displays information about eGTP-C P-GW ingress peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the P-GW ingress peer.
sgsn: Displays information about eGTP-C SGSN peers associated with the S4 service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the SGSN peer.
sgw-egress: Displays information about eGTP-C S-GW egress peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the S-GW egress peer.
sgw-ingress: Displays information about eGTP-C S-GW ingress peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the S-GW ingress peer.
address *ip_address*: Specifies the IP address of the selected peer in IPv4 dotted-decimal notation or IPv6 colon-separated notation.
wf1: Specifies that the output is to be displayed in wide format number 1.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information about eGTP-C peers associated with the service interface configured on this system. The output contains the following information about the peer:

- Status of the peer
- Echo status
- Restart counter status
- Peer restart counter knowledge
- Service ID
- Peer IP address
- Current sessions
- Maximum sessions

Important: The primary command, **show egtpc peers**, when entered without additional keywords, displays information for all peers associated with the service operating on this system.

Example

The following command returns an output for an eGTP-C S-GW egress peers associated with the service interface configured on this system with an IP address of *10.2.3.4*:

```
show egtpc peers interface sgw-egress address 10.2.3.4
```

The following command returns an output for an eGTP-C MME peer associated with the service interface configured on this system with an IP address of *10.2.3.4*:

```
show egtpc peers interface mme address 10.2.3.4
```

show egtpc sessions

Displays eGTP-C session information.

Product

P-GW, S-GW

Privilege

Inspector

Syntax

show egtpc sessions [egtp-service *name* **| interface { mme | pgw-ingress | sgsn | sgw-egress | sgw-ingress }] [| { grep** *grep_options* **| more }]**

---

egtp-service *name*

Displays information about eGTP-C sessions associated with an existing egtp-service specified as an alphanumeric string of 1 through 63 characters.

---

interface { mme | pgw-ingress | sgsn | sgw-egress | sgw-ingress }

Displays information about eGTP-C sessions associated with the service interface configured on this system.
mme: Displays information about eGTP-C sessions associated with the MME interface configured on this system.
pgw-ingress: Displays information about eGTP-C sessions associated with the P-GW ingress interface configured on this system.
sgsn: Displays information about eGTP-C sessions associated with the SGSN eGTP-C S4 interface configured on this system.
sgw-egress: Displays information about eGTP-C sessions associated with the S-GW egress interface configured on this system.
sgw-ingress: Displays information about eGTP-C sessions associated with the S-GW ingress interface configured on this system.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display session information for a specific eGTP service or for sessions associated with an interface type configured on this system.

Example

The following command displays eGTP-C session information for sessions associated with all P-GW ingress interfaces configured on this system:

```
show egtpc sessions interface pgw-ingress
```

The following command displays eGTP-C session information for sessions associated with all MME interfaces configured on this system:

show egtpc sessions interface mme

show egtpc statistics

Displays evolved GPRS Tunneling Protocol Control (eGTP-C) plane statistics for a specific service name or interface type.

Product

P-GW, S-GW

Privilege

Inspector

Syntax

show egtpc statistics [egtp-service *name* **| interface { mme | pgw-ingress | sgsn | sgw-egress | sgw-ingess } | mme-address** *ip_address* **| pgw-address** *ip_address* **| sgsn-address** *ip_address* **| sgw-address** *ip_address* **] [verbose] [| { grep** *grep_options* **| more }]**

egtp-service *name*

Displays statistics for an existing eGTP service specified as an alphanumeric string of 1 through 63 characters.

interface { mme | pgw-ingress | sgw-egress | sgw-ingess }

mme: Displays eGTP-C statistics for all MME interfaces.
pgw-ingress: Displays eGTP-C statistics for all eGTP P-GW ingress interfaces.
sgsn: Displays eGTP-C statistics for all eGTP S4 SGSN interfaces.
sgw-egress: Displays eGTP-C statistics for all eGTP S-GW egress interfaces.
sgw-ingress: Displays eGTP-C statistics for all eGTP S-GW ingress interfaces.

mme-address *ip_address*

Displays eGTP-C statistics for an existing MME IP address expressed in IPv4 dotted-decimal notation or IPv6 colon-separated notation.

pgw-address *ip_address*

Displays eGTP-C statistics for an existing P-GW IP address expressed in IPv4 dotted-decimal notation or IPv6 colon-separated notation.

sgsn-address *ip_address*

Displays eGTP-C statistics for an existing SGSN S4 IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated notation.

sgw-address *ip_address*

Displays eGTP-C statistics for an existing S-GW IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated notation.

verbose

Displays the maximum amount of detail available for this commands output. If this option is not specified, the output is truncated to a more concise level.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display evolved GPRS Tunneling Protocol Control (eGTP-C) plane statistics for a specific service name or interface type.

Example

The following command displays eGTP-C statistics for interfaces configured as S-GW ingress interfaces:

```
show egtpc statistics interface sgw-ingess
```

The following command displays eGTP-C session information for sessions associated with all MME interfaces configured on this system:

```
show egtpc sessions interface mme
```

show egtp-service

Displays configuration information for evolved GPRS Tunneling Protocol (eGTP) services on this system.

Product

MME, P-GW, S-GW

Privilege

Inspector

Syntax

show egtp-service { all | name *service_name* **} [| { grep** *grep_options* **| more }]**

all

Displays configuration information for all eGTP services configured on this system.

name *service_name*

Displays configuration information for an existing eGTP service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference Guide*.

Usage

Use this command to view configuration information for eGTP services on this system.

Example

The following command displays service statistics for the eGTP service named *egtp1*:

```
show egtp-service name egtp1
```

show event-notif server

Displays the counter information of configured Event Notification servers based on specific criteria.

Product

All

Privilege

Inspector

Syntax

```
show event-notif server all [ | {grep grep_options | more }]
```

all

Displays counter information for each active Event Notification server in this context.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display the counters pertaining to the Event Notification collection servers configured in a context.

Example

The following command displays the counter information for all Event Notification collection servers configured in a context:

```
show event-notif server all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show event-notif statistics

Displays the statistical information collected over configured Event Notification interface based on specific criteria.

Product

All

Privilege

Inspector

Syntax

```
show event-notif statistics [ | {grep grep_options | more }]
```

| { grep *grep_options* | more }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display the statistical information collected over configured Event Notification interface based on specific criteria.

Example

The following command displays the counter information for all Event Notification collection servers configured in a context:

```
show event-notif statistics
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show external-inline-servers

This command is obsolete.

show fa-service

Displays information on configured foreign agent (FA) services.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show fa-service { all | name *fa_name* **} [| { grep** *grep_options* **| more }]**

---

all | name *fa_name*

all: indicates information on all foreign agent services is to be displayed.
name *fa_name*: indicates only the information for the named FA service is to be displayed.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Display foreign agent service configuration information.

Example

The following commands display information on the FA service *sampleService* and all services, respectively.

```
show fa-service name sampleService

show fa-service all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show fans

Displays the current control status, speed, and temperature for the upper and lower fans in the system chassis.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show fans [| { grep *grep_options* **| more }]**

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

View the fan information to verify system hardware status as necessary.

Example

The following command displays information regarding the cooling fans in the system:

```
show fans
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show file

Displays the contents of the file specified. The contents are paginated as if it were normal ASCII output.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show file url *url* **[| { grep** *grep_options* **| more }]**

url *url*

Specifies the location of a file to display. *url* may refer to a local or a remote file. *url* must be entered using the following format:
[file:]{ /flash | /pcmcia1 | /hd }[/*directory* **]/***file_name*
tftp://{ *host***[** *:port#* **] }[/***directory* **]/***file_name*
[http: | ftp: | sftp:]//[*username***[** *:password* **]@] { ***host* **}[** *:port#* **][/***directory* **]/***file_name*

Important: Use of the SMC hard drive is not supported in this release.

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Display the contents of files to view such information as log data, trace information, etc.

Example

The following will display the contents of the local file */pub/log.txt*.

```
show file //pcmcia1/pub/log.txt
```

The following command will display the contents of the file */pub/log.txt* on remote host *remoteABC*.

show file ftp://remoteABC/pub/log.txt

show firewall flows

This command is obsolete.

show firewall ruledef

This command is obsolete.

show firewall statistics

This command is obsolete.

show fng-service

Displays information about specified Femto Network Gateway (FNG) service configuration, status, and counters, and includes information about all the sessions currently maintained by the FNG.

Product

FNG

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show fng-service { all [counters] | name *service_name* **| session | statistics }**

all

Displays information for all configured FNG services.

counters

Displays counters associated with the FNG service.

name *service_name*

Displays information only for an existing FNG service specified as an alphanumeric string of 1 through 63 characters.

session

Displays information about configured FNG sessions.

Important: See **show fng-service session** for detailed options.

statistics *service_name*

Total of collected information for specific protocol since the last **restart** or **clear** command.

Important: See **show fng-service statistics** for detailed options.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the section *Regulating a Command's Output* in the chapter *Command Line Interface Overview* in the *Command Line Interface Reference*.

Usage

Use this command to view information for selected configured FNG services.

Example

The following command displays available information for all active FNG services.

```
show fng-service all
```

Important: Command output descriptions are available in the *Statistics and Counters Reference*.

show fng-service session

Displays statistics for specific Femto Network Gateway (FNG) sessions.

Product

FNG

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show fng-service session [all | callid *call_id* **| counters | full [all | callid** *call_id* **| ip-address** *ip-address* **| peer-address** *ip_address* **| username** *name* **] | ip-address** *ip-address* **| peer-address** *ip-address* **| summary [all | callid** *call_id* **| ip-address** *ip-address* **| peer-address** *ip-address* **| username** *name* **] | username** *name* **]**

all

Displays all related information for all active FNG sessions.

callid

Displays PPP information for the call ID specified as a 4-digit hexadecimal number.

counters

Displays counters for the configured FNG sessions.

full

Displays all available information for the associated display or filter keyword.

ip-address *ipv4_address*

Displays information for the subscriber IP address specified in IPv4 dotted-decimal notation.

peer-address *ipv4_address*

Displays information for the IP peer specified by its IP address in IPv4 dotted-decimal notation.

summary

Displays summary information for FNG sessions.

username *user_name*

Displays information for a username within the current context specified as an alphanumeric string of 1 through 127 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the section *Regulating a Command's Output* in the *Command Line Interface Overview* chapter.

Usage

Use this command to view configuration information for an FNG session.

Example

The following command displays all available FNG sessions.

```
show fng-service session all
```

Important: Command output descriptions are available in the *Statistics and Counters Reference*.

show fng-service statistics

Displays statistics for the FNG since the last restart or clear command. The output includes the number of each type of protocol message. For example, the output includes the various types of EAP messages.

Product

FNG

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show fng-service statistics [name *service_name* **| peer-address** *ipv4_address* **]**

name *service_name*

Displays statistics for an existing service name specified as an alphanumeric string of 1 through 63 characters.

peer-address *ipv4_address*

Displays statistics for an IP peer specified by its IP address in IPv4 dotted-decimal notation.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the section *Regulating a Command's Output* in the *Command Line Interface Overview* chapter.

Usage

Use this command to display FNG statistics.

Important: You may use more than one keyword per command line.

Example

The following command displays information about the FNG service.

```
show fng-service statistics
```

Important: Command output descriptions are available in the *Statistics and Counters Reference.*

show freeze-ptmsi imsi

Displays the P-TMSI (packet-temporary mobile subscriber identify) corresponding to the IMSI (international mobile subscriber identity) that has entered a frozen state after the purge timeout timer expires.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show freeze-ptmsi imsi *imsi_num*

imsi *imsi_num*

Specifies the IMSI that has been frozen as a sequence of up to 15 digits. The first three digits are the MCC (mobile country code). The next two or three digits are the MNC (mobile network code). The remaining digits are the MSIN (mobile station identification number).

Usage

This command enables the operator to know whether a frozen IMSI has an associated P-TMSI.

Example

The following command displays the P-TMSI corresponding to a frozen IMSI:

```
show freeze-ptmsi imsi 262090426000194
```

show ggsn-service

Displays configuration information for Gateway GPRS Support Node (GGSN) services on the system.

Product

GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ggsn-service { all | name *ggsn_svc_name* **} [| { grep** *grep_options* **| more }]**

all

Displays information for all GGSN services configured with the given context.

name *ggsn_svc_name*

Displays information for an existing GGSN service name specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference*.

Usage

This command is used to verify the configuration of one or all GGSN services for monitoring or troubleshooting purposes. The output is a concise listing of GGSN service parameter settings.
If this command is executed from within the local context with the all keyword, information for all GGSN services configured on the system will be displayed.

Example

The following command displays configuration information for a GGSN service called *ggsn1*:

```
show ggsn-service name ggsn1
```

show ggsn-service sgsn-table

Lists all Serving GPRS Support Nodes (SGSNs) by IP addresses and shows the current number of subscribers to each SGSN.

Product

GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show ggsn-service sgsn-table
```

Usage

While there are existing commands to show SGSN subscriber information, this command is the only way to list all SGSNs by IP address and show the current number of subscribers to each SGSN.

Example

The following command will bring up a table showing the current active/inactive status, IP address, reboots/restarts and SGSN users.

```
show ggsn-service sgsn-table
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show global-title-translation

Displays configuration information for Global Title Translation (GTT).

Product

SGSN

Privilege

Inspector

Syntax

```
show global-title-translation { address-map { all | instance instance } | association {
all | instance instance } }
```

address-map { all | instance }

Displays configuration information for either the entire GTT address map database or for a specific instance of an address map. *instance* is an integer from 1 to 4096 which uniquely identifies the address map configuration.

association { all | instance }

Displays configuration information for either the entire database of GTT association lists for for a specific instance of GTT association configuration. *instance* is an integer from 1 to 16 which uniquely identifies the GTT association configuration.

Usage

This command displays the configuration for the GTT address maps and associations.

Example

The following command displays the address map *2047*.

```
show global-title-translation address-map 2047
```

show gmm-sm statistics

Displays statistics for the GPRS Mobility Management and Session Management (GMM/SM) configuration of the system's SGSN service. GMM/SM supports mobility to allow the SGSN to know the location of a Mobile Station (MS) at any time and to activate, modify and deactivate the PDP sessions required by the MS for user data transfer.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show gmm-sm statistics [ gmm-only | plmn-id mcc mcc mnc mnc [ access-type { gprs | umts } ] | sm-only ] [ gprs-service srvc_name | iups-service srvc_name | sgsn-service srvc_name ] [ verbose ] [ | { grep grep_options | more } ]
```

Keywords are presented below. Primary keywords are listed in the order of selection as shown in the syntax. Secondary or filtering keywords are presented alphabetically after the description of the primary keywords.

gmm-only

Displays only GPRS mobility management (GMM) information for other specified keyword parameters for the current context.

plmn-id mcc *mcc* **mnc***mnc* **[access-type { gprs | umts }]**

Filters the statistics display per PLMN.
Enter the **access-type** keyword to fine-tune the display of the GMM/SM statistics to an aggregate of the IuPS (select access-type UMTS) and/or the GPRS (select access-type GPRS) services belonging to the PLMN.

sm-only

Displays only session management (SM) information for other specified keyword parameters for the current context.

gprs-service *srvc_name*

Displays the statistics for an existing 2.5G GPRS service name specified as an alphanumeric string of 1 through 63 characters.
The display request can be narrowed by adding either the **nsei** or **routing-area** filter keywords.

iups-service *srvc_name*

Displays the statistics for an existing IuPS service specified as an alphanumeric string of 1 through 63 characters.
The display request can be narrowed by adding either the **rnc** or **routing-area** filter keywords.

sgsn-service *srvc_name*

Displays the statistics for an existing 3G SGSN service specified as an alphanumeric string of 1 through 63 characters.
The display request can be narrowed by adding either the **rnc** or **routing-area** filter keywords.

access-type *type*

Filters the display of service statistics by 2.5G GPRS services or 3G IuPS services for UMTS:

- **gprs**
- **umts**

If this keyword is not included, then statistics for both access types are displayed.

lac *lac_id*

Specifies the location area code (LAC) as part of the identification of the RNC or RA as an integer from 1 through 65535.

mcc *mcc_id*

Specifies the mobile country code (MCC) as part of the identification of the RNC or RA an integer from 100 through 999.

mnc *mnc_id*

Specifies the mobile network code (MNC) as part of the identification of the RNC or RA as a 2- or 3-digit integer from 00 through 999.

nsei *nse_id*

Displays the GMM/SM session statistics for an existing network service entity (NSEI) specified as an integer from 0 to 65535.

rac *rac_id*

Specifies the routing area code (RAC) as part of the identification of the RNC or RA as an integer from 1 through 255.

rnc *rnc_id*

Enter this keyword to fine-tune the display of the GMM/SM session statistics just for the radio network controller (RNC) specified as an integer from 0 through 4095.

routing-area mcc *mcc_id* **mnc** *mnc_id* **lac** *lac_id* **rac** *rac_id*

Enter the **routing-area** keyword to fine-tune the display of the GMM/SM statistics for a specified routing area (RA) identified by the MCC, MNC, LAC and RAC.

verbose

Displays all possible statistics for specified command or keyword.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display usage statistics for the GMM/SM session configurations for SGSN services, including a BSC attaches, activations, and throughput.

Example

The following command displays GMM/SM statistics for a specific routing area defined for the 2.5G SGSN's GPRS service:

```
show gmm-sm statistics gprs-service gprs1 routing-area mcc 123 mcc 131
lac 24 rac 11
```

The following command displays all possible information for GMM/SM statistics:

```
show gmm-sm statistics verbose
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show gprsns statistics

Displays the statistics for the 2.5G SGSN's GPRS NS layer (link level).

Product

SGSN

Privilege

Inspector

Syntax

```
show gprsns statistics { msg-stats { consolidated nse nse_id | nse nse_id } | sns-msg-stats } | { grep grep_options | more }
```

msg-stats

Displays the transmit (Tx) and receive (Rx) message statistics (except for SNS messages) in the statistics output.

consolidated nse *nse_id*

nse_id: Enter an integer from 0 to 65535.

nse *nse_id*

Display statistics for a NSE specified as an integer from 0 to 65535.

sns-msg-stats

Display subnetwork service (SNS) sublayer message statistics.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

This command is used to display Frame Relay statistics configured for the NSE/NSVC with the commands documented in the *Network Service Entity - Peer NSEI Configuration Mode Commands* chapter.
Collected statistics are cleared (deleted) with the **clear gprsns statistics** described in the *Exec Mode Commands (A-C)* chapter.

Example

Use the following command to display the collected message statistics for NSEI *1422*:

```
show gprsns statistics msg-stats nse 1422
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show gprsns status

Displays the status of the network service virtual circuits (NSVC) for the GPRS NS layer (link level).

Product

SGSN

Privilege

Inspector

Syntax

```
show gprsns status { nsvc-status-all nse nse_id | nsvc-status-consolidated nse nse_id |
nsvc-status-per-bvci bvci bvc_id nse nse_id } | { grep grep_options | more }
```

nsvc-status-all nse { all | nse*nse_id* **}**

Displays status information for all NSVCs included in the NSE specified as an integer from 0 to 65535.

nsvc-status-consolidated nse *nse_id*

nsvc-status-per-bvci bvci *bvc_id* **nse** *nse_id*

bvc_id is an integer from 0 to 65535.
nse_id is an integer from 0 to 65535.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

This command is used to display the status of the NSVC.

Example

Use the following command to display status of all NSVC for NSE 1422:

```
show gprsns status nsvc-status-all nse 1422
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show gprs-service

Displays the statistics for GPRS services.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show gprs-service { all | name *gprs_srvc_name* **} [| { grep** *grep_options* **| more }]**

all

Displays information for all GPRS services configured with this context.

name *gprs_srvc_name*

Displays information for an existing GRPS service name specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For more information on the usage of **grep** and **more**, refer to the Regulating a Command's Output section of the Command Line Interface Reference.

Usage

This command is used to verify the configuration of one or all GPRS services for monitoring or troubleshooting purposes. The output is a concise listing of GPRS service parameter settings.
If this command is executed from within the local context with the all keyword, information for all GPRS services configured on the system will be displayed.

Example

The following command displays configuration information for all GPRS services configured in this context:

```
show gprs-service all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show gprsssf

Displays statistics for various 3GPP Customised Applications for Mobile network Enhanced Logic (CAMEL) service GPRS Service Switching Function (gprsSSF) entities.

Product

SGSN

Privilege

Inspector

Syntax

show gprsssf { counters | statistics } [camel-service *srvc_name* **| gprs [2g-sgsn-app | 3g-sgsn-app] | gsmscf-address {** *address* **| all } | sms] [| { grep | more }]**

counters

Displays collected status counter information for CAMEL service entities.

statistics

Displays collected statistics for CAMEL service entities.

camel-service *srvc_name*

Filters the display of counters and statistics for an existing CAMEL service name in the SGSN configuration specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

gprs [2g-sgsn-app | 3g-sgsn-app]

Filters the counter/statistic output to display GPRS protocol information specific to either the 2.5G or 3G SGSN.

gsmscf-address { *address* **| all }**

The GSM service control function (gsmSCF) address is the ISDN address of the SCP where the CAMEL service resides. It is possible to display information for one or all of the configured CAMEL services. *address* is a standard ISDN E.164 address of 1 to 15 digits.

sms

Filters the display of counters and statistics for SMS protocol information.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to display CAMEL service status counter information and statistics collected since the last restart or clear command. If filters are not included with the command, then all statistics or counters are displayed for all CAMEL services in all contexts in which CAMEL services have been defined.
Collected statistics are cleared (deleted) with the **`clear gprsssf statistics`** command described in the chapter *Exec Mode Commands (A-C)*.

Example

Use the following command to display the status counter totals of the GPRS Dialogue parameters for a 3G SGSN:

```
show gprsssf counter gprs 3g-sgsn-app
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show gs-service

Displays configuration information and statistics for Gs services configured on system.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show gs-service { all | name *svc_name* **} [| { grep** *grep_options* **| more }]**

all

Displays information for all Gs services configured with in the given context.

name *svc_name*

Displays information for an existing Gs service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For more information on the usage of **grep** and **more**, refer to the Regulating a Command's Output section of the Command Line Interface Reference.

Usage

This command is used to verify the configuration of one or all Gs services for monitoring or troubleshooting purposes.
If this command is executed from within the local context with the all keyword, information for all Gs services configured on the system will be displayed.

Example

The following command displays configuration information for all Gs services configured on a system:

```
show gs-service all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show gtpc

Displays GPRS Tunnelling Protocol-Control (GTPC) information for GTPv0, GTPv1-C, GTPv1-U with filtering options.

Product

GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show gtpc [**full** | **counters** | **summary**] { **all** | **apn** *apn_name* | **imsi***imsi_value* [**nsapi** *nsapi_value*] | **callid** *callid* | **sgsn-address** *ip_address* | **ggsn-service** *ggsn_name* | **user-address** *ip_address* | **username** *username* }

[full | counters | summary]

Specifies the level of information to be displayed. The following levels can be used:

- **full**: Indicates detailed information is to be displayed.
- **counters**: Indicates the output is to include the statistical counters.
- **summary**: Indicates only summary information is to be displayed.

{ all | apn *apn_name* **| imsi** *imsi_value* **[nsapi** *nsapi_value* **] | callid** *callid* **| sgsn-address** *ip_address* **| ggsn-service** *ggsn_name* **| user-address** *ip_address* **| username** *username* **}**

Specifies the filter criteria used when displaying GTP information. The following filters can be used:

- **all**: Specifies that all available information is to be displayed.
- **apn** *apn_name*: Specifies that GTP information for an APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.
- **imsi** *imsi_value* **[nsapi** *nsapi_value* **]**: Displays GTP information for an International Mobile Subscriber Identity (IMSI) specified as an integer from 1 through 15 characters. Optionally, the IMSI could be further filtered by specifying a particular PDP context using the Network Service Access Point Identifier (NSAPI) expressed as an integer from 5 through 15.
- **callid** *callid*: Displays GTP information for a call identification number specified as a 4-digit hexadecimal number.
- **sgsn-address** *ip_address*: Displays GTP information for an SGSN specified by its IP address in IPv4 dotted-decimal notation.
- **ggsn-service** *ggsn_name*: Displays GTP information for an existing GGSN service specified an alphanumeric string of 1 through 63 characters that is case sensitive.
- **user-address** *ip_address*: Displays GTP information for a user PDP context specified as an IP address in IPv4 dotted-decimal notation.
- **username** *username*: Displays GTP information for a username specified as an alphanumeric string of 1 through 127 characters (including wildcards '$' and '*') that is case sensitive.

Usage

This command displays statistics for every GTP message type based on the filter criteria. This information is useful for system monitoring or troubleshooting.

Example

The following command displays GTPC counters for a GGSN service named *ggsn1*:

```
show gtpc counters ggsn-service ggsn1
```

The following command displays GTPC full information:

```
show gtpc full
```

The following command displays GTPC summary information for a specific call identification number of *05f62f34*:

```
show gtpc summary callid 05f62f34
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show gtpc statistics

Displays GTPv0, GTPv1-C, GTPv1-U statistics with filtering options.

Product

GGSN, MSEG

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show gtpc statistics [[custom1 | custom2] [apn *apn_name* **| ggsn-service** *ggsn_service_name* **| mseg-service** *mseg_service_name* **| sgsn-address** *ipv4_address* **] [[verbose] format1] [| { grep** *grep_options* **| more }]**

custom1

Displays statistics of GTP-C messages for preservation mode and free of charge service.
This keyword is customer specific and license enabled. For more information, contact your Cisco sales representative.

custom2

Displays statistics for GTP-C messages related to overcharging protection on loss of radio coverage for a GGSN service.
This keyword is feature specific and license enabled. For more information, contact your Cisco sales representative.

apn *apn_name*

Displays GTP-C statistics for an existing APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

ggsn-service *ggsn_service_name*

Displays GTP-C statistics for an existing GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

mseg-service *mseg_service_name*

Important: This keyword is not supported in this release. For more information please contact your Cisco account representative.

Displays GTP-C statistics for an existing Mobile Service Edge Gateway (MSEG) specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

sgsn-address *ipv4_address*

Displays GTP statistics for an SGSN specified by its IP address in IPv4 dotted-decimal notation.

verbose

Displays detailed instead of concise statistics.

format1

Displays more detailed statistical breakouts.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

The information displayed by this command consists of session statistics such as the number of currently active sessions categorized by PDP context type, and statistics for every GTP message type. The statistics are cumulative.
If the verbose keyword is used, additional information will be displayed such as statistics for every type of error code.

Example

The following command displays verbose GTP statistics:

```
show gtpc statistics verbose
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show gtpp

Displays information on the GPRS Tunneling Protocol Prime (GTPP) for the selected charging gateway function (CGF) or GCDR storage server.

Product

GGSN, SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show gtpp [ accounting | counters { all | cgf-address | group } | group { all | name } |
statistics { cgf-address | group } | storage server { counters | group | local |
statistics | status | streaming} ] [ | { grep grep_options | more } ]
```

Usage

This command displays the GTPP related information for the selected CGF or the G-CDRs storage server. If this command is issued from within the local context, information for all GTPP accounting servers configured on the system is displayed regardless of context.

Example

The following command displays the GTPP counters for all the servers:

```
show gtpp counters all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show gtpp accounting

Displays information on the GPRS Tunneling Protocol Prime (GTPP) accounting server configuration.

Product

GGSN, SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show gtpp accounting servers { group name group_name } [ | { grep grep_options | more } ]
```

Usage

This command is used to view the status of GTPP accounting servers configured within a context for monitoring or troubleshooting purposes.
If this command is issued from within the local context, information for all GTPP accounting servers configured on the system is displayed regardless of context.

Example

The following command displays the status of and information on configured GTPP accounting servers:

```
show gtpp accounting servers
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show gtpp counters

Displays GTPP counters for configured charging gateway functions (CGFs) within the given context.

Product

GGSN, SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show gtpp counters { all{ gcdrs } | cgf-address cgf_address | group name group_name } [ |
{ grep grep_options | more } ]
```

all

Displays counters for all CGFs configured within the context.

cgf-address *cgf_address*

Displays counters for a CGF specified by its IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Counters for a single CGF can be viewed using the **cgf-address** keyword. Counters for all CGFs in the context can be viewed by entering the command with the **all** keyword.
If this command is issued from within the local context and no CGF-address is specified, the counters displayed will be cumulative for all CGFs configured on the system regardless of context.

Example

The following command displays counters for all CGF:

```
show gtpp counters all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show gtpp group

Displays information pertaining to the configured GTPP storage server group.

Product

GGSN, SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show gtpp group [**name** *gtpp_group_name* | **all**] [| { **grep** *grep_options* | **more** }]

name *gtpp_group_name*

Displays information and CDR statistics for an existing GTPP server group name specified as an alphanumeric string of 1 through 64 characters.

all

Displays statistics for all configured GTPP storage server groups, including default group.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display the CDR statistics on the basis of GTPP server groups. It shows the information for all or specific GTPP server group configured in the context from which this command is issued.

Example

The following command displays the status of the GTPP server group backup server configured in a context called *GTPP_Group1*:

```
show gtpp group name GTPP_Group1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show gtpp statistics

Displays GTPP statistics for configured Charging Gateway Functions (CGFs) within the context.

Product

GGSN, SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show gtpp statistics [**cgf-address** *cgf_address* | **group name** *group_name*] [| { **grep** *grep_options* | **more** }]

cgf-address *cgf_address*

Displays statistics for a CGF specified by its IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated notation.

group name *group_name*

Displays server statistics information of an existing GTPP server group name specified as an alphanumeric string of 1 through 64 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Statistics for a single CGF can be viewed by specifying its IP address. Statistics for all CGFs in the context can be viewed by **not** specifying an IP address.
If this command is issued from within the local context, the statistics displayed will be cumulative for all CGFs configured on the system regardless of context.

Example

The following command displays statistics for a CGF with an IP address of *192.168.1.14*:

```
show gtpp statistics cgf-address 192.168.1.14
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show gtpp storage-server

Displays information pertaining to the configured GTPP storage server (GSS).

Product

GGSN, SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show gtpp storage-server [**counters** { **all** | **group name** *group_name* } | **group name** *group_name* | **local file** { **counters** { **all** | **group name** *group_name* } | **statistics** [**group name** *group_name*] } | **status** { **group name** *group_name* | **verbose** } | **streaming file** { **counters** { **all** | **group name** *group_name* } | **statistics** [**group name** *group_name*] }] [| { **grep** *grep_options* | **more** }]

counters

Displays counters for the external GTPP storage server.

group name *group_name*

Displays GTPP backup server information for the group name specified as an alphanumeric string of 1 through 64 characters.

local file

Displays statistics and counters for the local storage-server. This is the hard disk if hard disk support has been enabled with the **gtpp storage-server mode** command in the GTPP Group Configuration Mode.

statistics

Displays statistics for the GTPP storage server.

status [verbose]

Displays status of the GTPP storage server. **verbose** enables the detailed view.

streaming

Displays the status of Charging Data Record (CDR) backup on HDD while streaming mode is enabled.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Executing this command with no keywords displays status information for the GTPP backup server configured in the context from which this command is issued.

Example

The following command displays the GTPP CDR file statistics stored on the local SMC hard disk.

```
show gtpp storage-server local file counters all
```

The following command displays the status of the GTPP backup server configured in a context called ggsn1:

```
show gtpp storage-server
```

The following command displays statistics for the GTPP backup server configured in a context called ggsn1:

```
show gtpp storage-server statistics
```

The following command displays GCDR storage server counters:

```
show gtpp storage-server counters
```

The following command displays GCDR storage server status:

```
show gtpp storage-server status
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show gtpu statistics

Displays GPRS Tunneling Protocol user plane (GTP-U) statistics and counters on this system.

Product

P-GW, S-GW, MSEG

Privilege

Inspector

Syntax

show gtpu statistics [[gtpumgr-instance *instance_number* **] [gtpu-service** *gtpu_service_name* **| mseg-service** *mseg_service_name* **| peer-address** *ipv4/ipv6_address* **]] [| { grep** *grep_options* **| more }]**

gtpumgr-instance *instance_number*

Displays information for an existing GTP-U manager instance specified as an integer from 1 through 4294967295.

gtpu-service *gtpu_service_name*

Displays GTP-U statistics for an existing GTP-U service specified s an alphanumeric string of 1 through 63 characters.

mseg-service *mseg_service_name*

Important: This keyword is not supported in this release. For more information please contact your Cisco account representative.

Displays GTP-U statistics for an existing MSEG service specified as an alphanumeric string of 1 through 63 characters.

peer-address *ipv4/ipv6_address*

Displays GTP-U statistics and counters for an existing peer IP address specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference Guide*.

Usage

Use this command to view statistics and counters for GTP-U traffic on this system.

Example

The following command displays statistics for the GTP-U service named *egtp1*:

```
show egtpu statistics gtpu-service egtp1
```

show gtpu-service

Displays configuration information for GPRS Tunneling Protocol user plane (GTP-U) services on this system.

Product

P-GW, S-GW

Privilege

Inspector

Syntax

show gtpu-service { **all** | **name** *service_name* } [| { **grep** *grep_options* | **more** }]

all

Displays configuration information for all GTP-U services configured on this system.

name *service_name*

Displays configuration information for an existing GTP-U service specified an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference Guide*.

Usage

Use this command to view configuration information for GTP-U services on this system.

Example

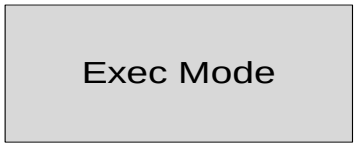
The following command displays service statistics for the GTP-U service named *egtp1*:

```
show egtp-service name egtp1
```

Chapter 116
Exec Mode Show Commands (H-L)

This section includes the commands **`show ha-service`** through **`show lte-policy`**.

The Exec Mode is the initial entry point into the command line interface system. Exec mode **show** commands are useful in troubleshooting and basic system monitoring.



show ha-service

Displays information on configured home agent services.

Product

HA

Privilege

Security Administrator Operator, Inspector

Syntax

show ha-service { all | name *ha_name* **} [| { grep** *grep_options* **| more }]**

---

all | name *ha_name*

all: Displays information on all Home Agent services is to be displayed.
name *ha_name*: Displays information for an existing HA service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Display home agent service configuration information.

Example

The following commands displays information on the HA service *sampleService* and all services, respectively.

```
show ha-service name sampleService

show ha-service all
```

show hardware

Displays information on the system hardware.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show hardware { card [*card_num* **] | inventory | version [board | diags | fans] } [| { grep** *grep_options* **| more }]**

card [*card_num* **]**

Provide the hardware information for all cards or the card specified by *card_num*. *card_num* must be a value in the range 1 through 48 and must refer to an installed card.

inventory

Display the hardware information for all slots in tabular format.

version [board | diags | fans]

Display the CPU information for all application cards and fan controller version for the upper and lower fan trays.
board: Only include the CPLD and FPGA version information.
diags: Only include the CFE diagnostics version information.
fans: Show the fan controller versions for the upper and lower fan trays.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Show the hardware information to verify part lists and hardware component versions with reserve stock

Example

The following displays the hardware information for a card installed in slot *1*.

```
show hardware card 1
```

The following command displays the hardware inventory for the entire chassis.

```
show hardware inventory
```

The following command results in the display of the CPU version for all application cards displaying only the CPLD and FPGA information.

```
show hardware version board
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show hd raid

Shows the output of the Redundant Array of Independent Disks (RAID) established on the SMCs.

Product

All

Privilege

Security Administrator, Administrator, Administrator, Operator

Syntax

```
show hd raid [ verbose ]
```

Example

```
show hd raid verbose
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show hd-storage-policy

Displays Array Configuration Replicator (ACR) counter and statistic information.

Product

HSGW, P-GW, S-GW

Privilege

Inspector

Syntax

show hd-storage-policy { all | counters [all] [name *name* **] [verbose] | name** *name* **| statistics [all] [name** *name* **] [verbose] }**

all

Displays ACR information for all HD storage policies configured on the system.

counters [all] [name *name* **] [verbose]**

all: Displays ACR counter information for all HD storage policies configured on the system.
name *name*: Displays ACR counter information for an existing HD storage policy specified as an alphanumeric string of 0 through 63 characters.

statistics [all] [name *name* **] [verbose]**

all: Displays ACR statistical information for all HD storage policies configured on the system.
name *name*: Displays ACR statistical information for an existing HD storage policy specified as an alphanumeric string of 0 through 63 characters.

verbose

Displays HD storage statistics based on instance.

Usage

Use this command to display ACR counter and statistic information.

Example

The following command displays ACR statistic information for an HD storage policy named *pgwsgw*:

```
show hd-storage-policy statistics name pgwsgw
```

show hnbgw access-control-db

Displays the white list of IMSI records in the Access Control database residing on Home-NodeB Gateway (HNB-GW) service instances that control HNB and UE access to HNB-GW sessions.

Product

HNB-GW

Privilege

Inspector

Syntax

show hnbgw access-control-db { hnbgw-service*hnbgw_svc_name* **| imsi** *imsi_value***}**

hnbgw-service *hnbgw_svc_name*

Displays Access Control database records for an existing HNB-GW service specified as an alphanumeric string of 1 through 63 characters.

imsi *imsi_value*

Specifies the International Mobile Subscriber Identification (IMSI) number which is found on the Access Control database for he HNB-GW service.
imsi_value is an integer consisting of the 3-digit MCC (Mobile Country Code), the 2- or 3-digit MNC (Mobile Network Code) followed by the MSIN (Mobile Subscriber Identification Number). The total IMSI value must not exceed 15 digits.

Usage

This command displays the white list IMSI records in an Access Control database residing on Home-NodeB Gateway (HNB-GW) service instances. The white list controls HNB and UE access to HNB-GW sessions. Access Control database records can be filtered by HNB-GW service or IMSI value.

Example

The following command displays the information for registered IMSIs and their status in the HNB-GW database named *hnbgw1*:

```
show hnbgw access-control-db hnbgw-service hnbgw1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show hnbgw counters

Displays the session counter information for Home-NodeB Gateway (HNB-GW) services connected on this system.

Product

HNB-GW

Privilege

Inspector

Syntax

show hnbgw counters [hnbgw-service *hnbgw_svc_name* **| hnbid** *hnb_identifier* **] [| { grep** *grep_options* **| more }]**

hnbgw-service *hnbgw_svc_name*

Filters the counter display based on an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

hnbid *hnb_identifier*

Filters the counter display based on a Home-NodeB identifier specified as an alphanumeric string of 1 through 255 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter.

Usage

Use this command to view the session counter information for HNB-GW services configured and HNBs connected on this system.

Example

The following command displays the counters for the HNB-GW service named *hnbgw1*:

```
show hnbgw counter hnbgw-service hnbgw1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show hnbgw sessions

Displays the active/dormant session information about registered HNB(s) on Home-NodeB Gateway (HNB-GW) service instances configured and running on this system based on different filter criteria.

Product

HNB-GW

Privilege

Inspector

Syntax

show hnbgw sessions [**full** | **summary**] [**all**] [**address** *hnb_ip_address* | **cell-id** *cell_id* | **hnb-access-mode** [**open** | **closed**] | **hnb-local-id** *hnb_id* | **hnbgw-service** *hnbgw_svc_name* | **hnbid** *hnb_glbl_id* | **mcc** *mcc* | **mnc** *mnc* [**lac** *lac* | **rac** *rac* | **rnc** *rnc*]] [| {**grep** *grep_options* | **more** }]

full

Displays the full information for a specific registered HNB session(s) on an HNB-GW service instance running on the system. The display can be filtered based on given filtering criteria.

summary

Displays summarized information for a specific registered HNB session(s) on an HNB-GW service instance running on the system. The display can be filtered based on given filtering criteria.

all

Displays summarized information for all registered HNB sessions on an HNB-GW service instance running on the system. The display can be filtered based on given filtering criteria.

address *hnb_ip_address*

Filters the display of full or summarized session statistics to show only HNB session(s) based on the registered HNB IP address expressed in IPv4 dotted-decimal notation.

cell-id *cell_id*

Filters the display of full or summarized session statistics to show only HNB session(s) based on the registered Femto cell ID where the user/subscriber is geographically located. and must be an integer from 0 through 268435455.*cell_id* is an integer from 0 through 268435455.

hnb-access-mode [open | closed]

Filters the display of full or summarized session statistics to show only HNB session(s) based on the HNB access mode in an HNB-GW service instance.

- **open** filters the session statistics for open HNBs connected with HNB-GW service instance in Open Access mode.
- **closed** filters the session statistics for closed HNBs connected with HNB-GW service instance in Closed Access mode.

hnb-local-id *hnb_id*

Filters the display of full or summarized session statistics to show only HNB session(s) based on the registered local ID of HNB specified as an integer from 1 through 25.

hnbgw-service *hnbgw_svc_name*

Filters the display of session statistics to show only registered HNB session(s) based on an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

hnbid *hnb_glbl_id*

Displays summarized or full information of HNB session(s) based on the registered global ID of HNB specified as an integer between 1 through 255.

mcc *mcc*

Displays summary information of HNB session(s) based on the registered Mobile Country Code (MCC) identification number of the UE specified as an integer between 101 through 999.

mnc *mnc*

Displays summarized or full information of HNB session(s) based on the registered Mobile Network Code (MCC) identification number of the UE specified as a 2- or 3-digit integer between 00 through 999.

lac *lac*

Displays summarized or full information for HNB session(s) based on the registered Location Area Code (LAC) identification number of the UE specified as an integer between 1 through 65535.

rac *rac*

Displays summarized or full information for HNB session(s) based on the registered Radio Access Code (RAC) identification number of the UE specified as an integer between 1 through 255.

rnc *rnc*

Displays summarized or full information for HNB session(s) based on the registered Radio Network Code (RAC) identification number of the HNB specified as an integer between 1 through 65535.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter.

Usage

Use this command to view the session statistics of all or specific registered HNB session(s) or in selected part of user session for HNB-GW services configured and running on this system.

Example

The following command displays summarized session statistics for all registered HNBs on the HNB-GW service named *hnbgw1*:

```
show hnbgw sessions summary hnbgw-service hnbgw1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show hnbgw statistics hnbgw-service

Displays the session statistics for Home-NodeB Gateway (HNB-GW) services configured and running on this system.

Product

HNB-GW

Privilege

Inspector

Syntax

```
show hnbgw statistics hnbgw-service hnbgw_svc_name [ hnbap-only | ranap-only | rua-only |
sccp-only | sctp-only ] [ verbose] [ | { grep grep_options | more } ]
```

hnbgw-service *hnbgw_svc_name*

Filters the display of session statistics for an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

hnbap-only

Filters the display of session statistics to show only Home NodeB Application Part (HNBAP) traffic for the selected HNB-GW service which is configured and running on this system.

ranap-only

Flitters the display of session statistics t to show only Radio Access Network Application Protocol (RANAP) traffic for the selected HNB-GW service which is configured and running on this system.

rua-only

Filters the display of session statistics to show only RANAP User Adaptation (RUA) traffic for the selected HNB-GW service which is configured and running on this system.

sccp-only

Filters the display of session statistics to show only Signaling Connection Control Part (SCCP) traffic for the selected HNB-GW service which is configured and running on this system.

sctp-only

Filters the display of session statistics to show only Stream Control Transmission Protocol (SCTP) traffic for selected HNB-GW service which is configured and running on this system.

verbose

Displays detailed statistics for all sessions on HNB-GW services or for a selected filtered and named HNB-GW service which is configured and running on this system.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter.

Usage

Use this command to view the session statistics for overall session or in selected part of user session for HNB-GW services configured and running on this system.

Example

The following command displays session statistics for the HNBAP part of session details for the HNB-GW service named *hnbgw1*:

```
show hnbgw statistics hnbgw-service hnbgw1 hnbap-only
```

The following command displays session statistics for the RANAP part of session with maximum details for the HNB-GW service named *hnbgw1*:

```
show hnbgw statistics hnbgw-service hnbgw1 ranap-only verbose
```

show hnbgw statistics hnbid

Displays the session statistics for Home-NodeB (HNB) connected to an HNB-GW service on this system.

Product

HNB-GW

Privilege

Inspector

Syntax

```
show hnbgw statistics hnbid hnb_identifier [ hnbap-only | ranap-only | rua -only] [
verbose] [ | { grep grep_options | more } ]
```

hnbid *hnb_identifier*

Filters the display of session statistics based on an existing Home-NodeB identifier specified as an alphanumeric string of 1 through 255 characters.

hnbap-only

Filters the display of session statistics display to show only Home NodeB Application Part (HNBAP) traffic for the selected HNB which is connected to this system through HNB-GW service.

ranap-only

Filters the display of session statistics display to show only Radio Access Network Application Protocol (RANAP) traffic for the selected HNB which is connected to this system through HNB-GW service.

rua-only

Filters the display of session statistics display to show only RANAP User Adaptation (RUA) traffic for the selected HNB which is connected to this system through HNB-GW service.

verbose

Displays detailed statistics for all HNB sessions or for the selected filter and HNB which is connected to this system through HNB-GW service.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter.

Usage

Use this command to view the session statistics for overall session or in selected part of user session for selected HNB which is connected to this system through HNB-GW service.

Example

The following command displays session statistics for the HNBAP part of session details for the HNB identified as *hnb112234* on this system:

show hnbgw statistics hnbid hnb112234 hnbap-only

The following command displays detailed session statistics for the RANAP part of session details for the HNB identified as *hnb112234* on this system:

show hnbgw statistics hnbid hnb112234 ranap-only verbose

show hnbgw-service

Displays the configuration details for configured HNB-GW service(s) on this system.

Product

HNB-GW

Privilege

Inspector

Syntax

```
show hnbgw-service { all | hnbgw-service hnbgw_svc_name }
```

all

Displays configuration and other default parameters for all HNB-GW service configured on this system.

hnbgw-service *hnbgw_svc_name*

Displays configuration and default parameters for an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to view the configuration and service parameters set for all or any specific HNB-GW service(s) on this system.

Example

The following command displays configuration parameters for all HNB-GW services configured on this system:

```
show hnbgw-service all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show hsgw-service

Displays information for HRPD Serving Gateway (HSGW) services on this system.

Product

HSGW

Privilege

Inspector

Syntax

show hsgw-service { all | name *service_name* **| statistics { all | name** *service _name* **} } [pcf-status [address** *IPv4_address* **| filter { all | icmp-monitored | no-calls | summary | up }] [| { grep** *grep_options* **| more }]**

---

all

Displays configuration information for all HSGW services configured on this system.

---

name *service_name*

Displays configuration information for an existing HSGW service specified as an alphanumeric string of 1 through 63 characters.

---

statistics

Displays node-level statistics for the HSGW.

---

pcf-status

Displays information about status of Packet Control Functions (PCFs) being monitored.

---

address *IPv4_address*

Displays status information for the specified PCF.
IPv4_address must be specified using IPv4 dotted-decimal notation.

---

filter { all | icmp-monitored | no-calls | summary | up }

Filters the PCF status information. Must be followed by the filter to be applied.
all: Shows all the PCFs.
icmp-monitored: Shows only PCFs which are ICMP monitored.
no-calls: Shows only PCFs which has no active sessions.
summary: Shows only a summary of the status of the PCFs.
up: Shows only PCFs which are alive.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the Regulating a Command's Output section of Chapter 1 of the Command Line Interface Reference Guide.

Usage

Use this command to view configuration information for HSGW services on this system.

Example

The following command displays service statistics for the HSGW service named *hsgw1*:

```
show hsgw-service name hsgw1
```

show hss-peer-service

Displays service, session, and statistics information for Home Subscriber Server (HSS) peer services configured on this system.

Product

MME

Privilege

Inspector

Syntax

show hss-peer-service { service { all | name *name* **} | session { all | callid** *id* **| full | mdn** *mdn* **| nai** *nai* **| summary } | statistics { all | service** *name* **| summary } } [| { grep** *grep_options* **| more }]**

service { all | name *name* **}**

Displays HSS peer service statistics for HSS peer services configured on this system.
all: Displays HSS peer service statistics for all configured HSS peer services on this system.
name *name*: Displays HSS peer service statistics for an existing HSS peer service specified as an alphanumeric string of 1 through 63 characters.

---

session { all | callid *id* **| full | mdn** *mdn* **| nai** *nai* **| summary }**

Displays HSS peer service statistics for sessions on this system.
all: Displays HSS peer service statistics for all sessions on this system.
This keyword is also used to further filter the **full** and **summary** options.
callid *id*: Displays summarized or detailed statistics of HSS peer service sessions running and filtered on the basis of the call identifier specified as an 8-digit hexadecimal number.
This keyword is also used to further filter the **full** and **summary** options.
mdn *mdn*: Displays summarized or detailed statistics of MME sessions running and filtered on the basis of an existing Mobile Directory Number (MDN) expressed as an alphanumeric string of 1 through 100 characters.
This keyword is also used to further filter the **full** and **summary** options.
nai *nai*: Displays summarized or detailed statistics of MME-HSS sessions running and filtered on the basis of an existing Network Access Identifier (NAI) expressed as an alphanumeric string of 1 through 128 characters.
This keyword is also used to further filter the **full** and **summary** options.
summary: Displays a summarized output of session information. This keyword can be further filtered by adding the following options:

- **full**
- **callid** *id*
- **mdn** *mdn*
- **nai** *nai*

---

statistics { all | service *name* **| summary }**

Displays statistics for HSS peer services configured on this system.
all: Displays statistics for all HSS peer services configured on this system.

service *name*: Displays statistics for a an existing HSS peer service expressed as an alphanumeric string of 1 through 63 characters.
summary: Displays summarized statistics for all HSS peer services configured on this system.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *CLI Overview* chapter of the *Command Line Interface Reference*.

Usage

Use this command to display service, session, and statistics information for HSS peer services configured on this system.

Example

The following command displays HSS peer service information and statistics for a session with a call ID of *08f11fa4*:

```
show hss-peer-service sessions full callid 08f11fa4
```

show imei-profile

Displays information for configured International Mobile Equipment Identity (IMEI) profiles.

Product

SGSN

Privilege

Inspector

Syntax

show imei-profile { all | full { all | name *imei_name* **} | name** *imei_name* **} [| { grep** *grep_options* **| more }]**

---

all

Lists all IMEI profiles configured on the system.

---

full { all | name *apn_name* **}**

full: Instructs the system to display all information in the IMEI profile(s).
all: Displays a full set of information for all IMEI profiles configured on the system.
name *imei_name*: Displays a full set of information for a specific IMEI profile.
apn_name: Must be an existing IMEI profile expressed as an alphanumeric string of 1 through 64 characters.

---

name *imei_name*

Displays information for a specific IMEI profile expressed as an alphanumeric string of 1 through 64 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information for IMEI profiles configured on the system. APN profiles are configured through the global configuration mode and in the IMEI profile configuration mode. For more information regarding IMEI profile commands, refer to the *IMEI Profile Configuration Mode Commands* chapter.

Example

The following command displays all available information for an IMEI profile named *imeiprof1*:

```
show imei-profile full name imeiprof1
```

show ims-authorization policy-control

Displays information and statistics specific to the policy control in IP Multimedia Subsystem (IMS) authorization service.

Product

SCM, GGSN, IMS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show ims-authorization policy-control statistics [ service ims_auth_svc_name | server {
ip-address ip_address [ port port_value ] | name server_name } ] [ | { grep grep_options
| more } ]
```

statistics

Displays the total collected statistics of all policy control parameters of IMS authorization service sessions since the last system **restart** or **clear** command.

service *ims_auth_svc_name*

Displays the total collected statistics of all IMS authorization sessions processed by a specific IMS authorization service since the last system restart or clear command. *ims_auth_svc_name* must be an existing IMS authorization service name, expressed as an alphanumeric string of 1 through 64 characters.

server { ip-address *ip_address* **[port** *port_value* **] | name** *server_name* **}**

Displays the server-level message statistics and the server IP address.
Specify the PCRF server name (1 through 64 alphanumeric characters), or server IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information and statistics about policy control configuration in existing IMS authorization services.

Example

The following command displays the existing IMS authorization service name *ims_auth_gx1* on the system:

```
show ims-authorization policy-control statistics service ims_auth_gx1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ims-authorization policy-gate

Displays information of installed Policy Gates for specific subscriber in an IP Multimedia Subsystem (IMS) authorization (IMSA) service.

Product

SCM, GGSN, IMS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ims-authorization policy-gate { { status [summary | full] [{ imsi *imsi_value* **[nsapi** *nsapi_value* **] } | callid** *call_id* **| { ims-auth-service** *ims_auth_svc* **} [rulename** *rule_name* **] } | { counters [all | { imsi** *imsi_value* **[nsapi** *nsapi_value* **] } | { rulename** *rule_name***} | { callid** *call_id* **}] } [| { grep** *grep_options* **| more }]]**

status [summary | full]

Displays the status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based on the specified criteria.
summary: Limits the display to a summary on the status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.
full: Displays the full information on status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.

counters all

Displays the counters/statistics of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.
all displays all counters of the installed gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.

imsi *imsi_value* **[nsapi** *nsapi_value* **]**

Displays all of the counters/status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based on the International Mobile Subscriber Identity (IMSI).
nsapi *nsapi_value* specifies the Network Service Access Point Identifier (NSAPI) and limits the display to a single PDP context of the subscriber.

callid *call_id*

Displays all of the counters/status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the call identifier.

ims-auth-service *ims_auth_svc*

Displays the status of the installed policy gates and their flow definitions along with their run-time status in the named IMS authorization service.

rulename *rule_name*

Displays all of the counters/status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the named dynamic charging rule.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Please refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference* for details on the usage of **grep** and **more**.

Usage

Use this command to display information/statistics/counters about all of the installed policy gates and their flow definitions along with the run-time status with specified criteria and filters in existing IMS authorization services.

Example

The following command displays the full status of the installed policy gates in an existing IMS authorization service on the system:

```
show ims-authorization policy-gate status full
```

The following command displays the all counters of the installed policy gates in an existing IMS authorization service on the system:

```
show ims-authorization policy-gate counters all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ims-authorization servers

Displays information and statistics specific to the authorization servers used for IP Multimedia Subsystem (IMS) authorization (IMSA) service.

Product

SCM, GGSN, IMS

Privilege

Security Administrator, Administrator

Syntax

show ims-authorization servers [ims-auth-service *ims_auth_svc_name* **[| { grep** *grep_options* **| more }]]**

server [ims-auth-service *ims_auth_svc_name* **]**

Displays the information and statistics for all authorization servers configured within an IMS authorization service in a system.
ims-auth-service *ims_auth_svc_name*: Displays the configured authorization servers for IMS authorization within the named IMS authorization service.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Please refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference* for details on the usage of **grep** and **more**.

Usage

Use this command to display information and statistics about IMS authorization servers configured on a system or IMS authorization service.

Example

The following command displays the information and statistics of the authorization servers in the IMS authorization service named in *ims_auth_gx1*:

```
show ims-authorization servers ims-auth-service ims_auth_gx1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ims-authorization service

Displays information, configuration, and statistics of all/specific IP Multimedia Subsystem (IMS) authorization (IMSA) service.

Product

SCM, GGSN, IMS

Privilege

Security Administrator, Administrator

Syntax

show ims-authorization service { { all [verbose] | name *ims_auth_svc_name* **| summary] } | { statistics [all | name** *ims_auth_svc_name* **] [verbose] } [| { grep** *grep_options* **| more }] }**

---

all [verbose]

Displays information and configuration for all configured IMS authorization services with a single line of information for each IMS authorization service.
verbose: Displays all information and configuration data for all IMS authorization services configured on system.

---

name *ims_auth_svc_name* **]**

Displays the information, statistics, and configuration data for the named IMS authorization service.

---

summary

Displays summarized information and configuration data for all IMS authorization services configured in a system.

---

statistics [all | name *ims_auth_svc_name* **] [verbose]**

Displays the IMS Authorization service statistics including following information:

- Initial authorization procedures
- Re-authorization procedures initiated by us
- Re-authorization procedures initiated by servers
- Various failure statistics

If no criteria are specified, only summarized statistics for all IMS Authorization services are displayed

- **all**: displays individual statistics for every IMS authorization service configured on system.
- name *ims_auth_svc_name*: Displays the statistics for the IMS authorization service named in *ims_auth_svc_name*
- verbose: displays detailed statistics for a configured IMS authorization service.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Please refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference* for details on the usage of **grep** and **more**.

Usage

Use this command to display the status, counters and configuration. for an IMS Authorization service. The status includes the state of a server table switchover. The Statistics option displays information about various processes.

Example

The following command displays the information and configuration data of the IMS authorization service named in *ims_auth_gx1*:

```
show ims-authorization service name ims_auth_gx1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ims-authorization sessions

Displays information, configuration, and statistics of sessions active in an IP Multimedia Subsystem (IMS) authorization (IMSA) service.

Product

SCM, GGSN, IMS

Privilege

Security Administrator, Administrator

Syntax

show ims-authorization session [**full** | **summary** | **ggsn-only**] | [**all** | [**ims-auth-service** *ims_auth_svc_name* | **imsi** *imsi_value* [**nsapi** *nsapi_value*] | **apn** *apn_name* | **ip-address** *ip_address* | **callid** *call_id*] [| { **grep** *grep_options* | **more** }]]

full

Displays complete information and configuration data for all sessions in IMS authorization services configured in a system.

summary

Displays summarized information and configuration data for all sessions in IMS authorization services configured in a system.

ggsn-only

Displays GGSN-specific information in addition to detailed information about the session.

all

Displays information and configuration for all sessions running in IMS authorization services with a single line of information for each IMS authorization session.

ims-auth-service *ims_auth_svc_name* **]**

Displays the information, statistics, and configuration data for sessions in the named IMS authorization service.

imsi *imsi_value* **[nsapi** *nsapi_value* **]**

Displays all of the counters/status of the running services in an IMS authorization service based on the specified International Mobile Subscriber Identity (IMSI) and Network Service Access Point Identifier (NSAPI). The display is limited to a single PDP context of the subscriber.

apn *apn_name*

Displays all of the counters/status for the running services in an IMS authorization service based on the specified Access Point Name (APN).

ip-address *ip_address*

Displays all of the counters/status for the running services in IMS authorization service based on the specified host IP address.

callid *call_id*

Displays all of the counters/status for the running services in IMS authorization service based on the named call identifier.

summary

Displays summarized information and configuration data for all IMS authorization services configured in a system.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Please refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference* for details on the usage of **grep** and **more**.

Usage

Use this command to display the sessions running under IMS Authorization service on a system with different filter criteria.

Example

The following command displays the information and statistical data for a session in an IMS authorization service:

```
show ims-authorization sessions full
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ip

Displays information for the IP-based interface access group and access control list (ACL) along with the address resolution protocol (ARP) information for the current context.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ip { access-group [*statistics*] **| access-list [** *list_name* **] | arp [** *arp_ip_address* **] | [summary] | statistics]] | localhosts [** *host_name* **] | prefix-list [detail [** *list_name* **] | name** *list_name* **| summary [** *list_name* **]] | rip | route [** *route_ip_address* **[** *route_gw_address* **]] | static-route** *sroute_ip_address* **[** *sroute_gw_address* **] | vrf** *vrf-name***} [| { grep** *grep_options* **| more }]**

access-group [*statistics* **]**

Displays all configured access groups in the current context along with their priority values.
statistics: Displays all configured access groups along with packet and byte counters for each ACL rule hit for the current context. It also shows the priority values.

access-list [*list_name* **]**

Indicates the output is to display the information for all ACLs or the named ACL.

arp [*arp_ip_address* **]**

Displays the ARP table or the ARP information associated with the IP address specified using IPv4 dotted-decimal or IPv6 colon-separated notation.

Important: When it restarts, the VPN Manager removes all interfaces from the kernel; the kernel then removes all ARP entries. When this happens, the NPU still holds all of the ARP entries so that there is no traffic disruption. From a user point of view, **show ip arp** is broken since this command gathers information from the kernel and not the NPU.

localhosts [*host_name* **]**

Displays all the local host information or only for the named host.

prefix-list [detail [*list_name* **] | name** *list_name* **| summary [** *list_name* **]]**

Displays information on configured IP prefix lists. With no keyword supplied, a list of all prefix lists and their entries is displayed.
detail [*list_name* **]**: Lists detailed information for all prefix lists and their entries. If a list name is specified only the details for the specified prefix list are displayed. *list_name* is an alphanumeric string of 1 through 79 characters.
name *list_nam*: Lists the entries for an existing prefix list specified as an alphanumeric string of 1 through 79 characters.

summary [*list_name* **]**: Lists summary information for all prefix lists and their entries. If a list name is specified, only the summary for the specified prefix list are displayed. *list_name* is an alphanumeric string of 1 through 79 characters.

---

rip

Displays general Routing Information Protocol (RIP) routing process information. (RIP is not supported at this time.)

---

route [*route_ip_address* **[** *route_gw_address* **]]**

displays the route information to the specified IP address. The route gateway address may be specified as needed to identify the route. The IP addresses are specified using tIPv4 dotted-decimal or IPv6 colon-separated notation.

---

static-route *sroute_ip_address* **[** *sroute_gw_address* **]**

Displays the static route information for the specified IP address. The static route gateway address may also be specified to identify the route. the IP addresses are specified using IPv4 dotted-decimal or IPv6 colon-separated notation.

---

vrf *vrf_name*

Displays Virtual Routing and Forwarding (VRF) information for the named VRF.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Show the IP information to verify and/or troubleshooting communication difficulties between to a remote host/node.

Example

The following command displays the ACL for the list named *sampleACL*.

```
show ip access-list sampleACL
```

The following command will output the static route information to remote host *10.2.3.4*.

```
show ip static-route 10.2.3.4
```

show ip as-path-access-list

Displays the contents of a Border Gateway Protocol (BGP) router Autonomous System (AS) path access list in the current context.

Product

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ip as-path-access-list *list_name*

list_name

Specifies the name of an existing AS path access list configured in the current context as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to display the configured entries for the specified BGP router AS path access list in the current context.

Example

The following command displays the contents of an AS path access list named *ASlist1*:

```
show ip as-path-access-list ASlist1
```

show ip bgp

Displays Border Gateway Protocol (BGP) information for the current context.

Product

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ip bgp [*ip_address/mask* **| debugging | filter-list** *list_name* **| neighbors [** *ip_adrress* **] | route-map** *map_name* **| vpnv4 { all [network | neighbors | summary] | vrf vrf-name [network] | route-distinguisher [network | neighbors | summary] } [| { grep grep_options | more }]**

ip_address/mask

Specifies the IP address and netmask bits for the network for which information should be displayed. The IP address and mask is the number of subnet bits, representing a subnet mask in CIDR notation. These must be entered in the IPv4 dotted-decimal or IPv6 colon-separated CIDR notation.

debugging

Displays debug flags that are enabled.

filter-list *list_name*

Displays routes that match the specified filter list.

neighbors [*ip_address***]**

Displays information for all neighbors or a neighbor specified as an IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.

route-map *map_name*

Displays routes that match the specified route-map.

vpnv4 { all [network | neighbors | summary] | vrf *vrf-name* **[network] | route-distinguisher [network | neighbors | summary] }**

Displays all VPNv4 routing data, routing data for a VRF, or a route-distinguisher.

- **all**: Displays all VPN routing information. If this is specified, the information displayed is gathered from all the VRF's known to BGP and displayed. It could contain the list of neighbors, the list of networks, or a particular network
- **network**: Displays the network for which information in the BGP routing table.
- **neighbors**: Displays neighbor information for the all the VRFs including the default VRF or for the VRF with a matching RD value.
- **summary**: Displays summary information of neighbors for all the VRFs including the default VRF or for the VRF with a matching RD value.

- **vrf** *vrf name*: Displays information only gathered from the named VRF. If there is no such VRF, an error is reported.
- **network**: Displays the network for which information in the BGP routing table.
- **route-distinguisher**: If specified along with the RD value, the information displayed is gathered from the corresponding VRF whose RD value is the same as the specified value. If there is no VRF associated with such an RD, an error is reported.
- **network**: Displays the network for which information in the BGP routing table.
- **neighbors**: Displays neighbor information for the all the VRFs including the default vrf VRF for the VRF with a matching RD value.
- **summary**: shows summary information of neighbors for all the vrfs including the default vrf or for the VRF with a matching RD value.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command display to BGP information for the current context.

Example

The following command displays information for all BGP neighbors:

```
show ip bgp neighbors
```

show ip interface

Displays statistical and configuration information for the IP-based interfaces, including a Virtual Routing and Forwarding (VRF) table for a specific context.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ip interface [vrf *vrf-name* **] [name** *intfc_name* **[statistics] [tunnel [gre-keepalive]] [summary] [| { grep** *grep_options* **| more }]**

vrf *vrf_name*

Displays Virtual Routing and Forwarding (VRF) routing information for an existing VRF specified as an alphanumeric string of 1 through 63 characters.

name *intfc_name*

Displays information for an existing interface specified as an alphanumeric string of 1 through 79 characters. If no interface name is specified, the information for all IP interfaces is displayed.

tunnel [gre-keepalive]

Filters the IP interface information for GRE/IP-in-IP tunnel type interfaces.
gre-keepalive: Displays the keepalive information for a generic routing encapsulation (GRE) tunnel configured with this IP interface.

statistics

Displays the session statistics of all ingress and egress packets processed through this IP interface.

summary

Displays summarized information about requested IP interfaces.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display the summarized of detailed configuration and statistical information for a configured IP interface. This information can be used to verify and/or troubleshoot communication difficulties between to a remote host/node.

Example

The following command displays the interface information, including statistics, for the IP interface *sampleInterface*.

show ip interface sampleInterface statistics

The following command displays the GRE keepalive information for an IP interface named in *IP_gre1*.

show ip interface IP_gre1 unnel gre-keepalive

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ip ospf

Displays Open Shortest Path First (OSPF) routing information.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ip ospf [border-routers | database [verbose] [ls-id *ip_addr* **] [adv-router** *ip_addr* **] [ls-type { router | network | summary | asbr-summary | external | nssa |** *integer* **}] | debugging | interface | neighbor [details] | route | virtual-links]**

---

border-routers

Displays all known area border routers (ABRs) and autonomous system border routers (ASBRs) for OSPF.

---

database [verbose] [ls-id *ip_addr* **] [adv-router** *ip_addr* **] [ls-type { router | network | summary | asbr-summary | external | nssa |** *integer* **}]**

Displays a summary of the database information for OSPF.
verbose: Displays detailed OSPF database information.
ls-id *ip_addr*: Displays OSPF database information for the link state advertisements (LSAs) with the specified link state identifier (LSID). *ip_addr* is entered using IPv4 dotted-decimal notation.
adv-router *ip_addr*: Displays OSPF database information for the advertising router with the specified LSID. *ip_addr* is entered using IPv4 dotted-decimal notation.
ls-type { router | network | summary | asbr-summary | external | nssa | *LSA_Numerical_Type* **}]**: Displays OSPF database information for the specified LSA type.

---

debugging

Lists which debugging parameters are enabled.

---

interface

Displays interface information for OSPF.

---

neighbor [details]

Displays summarized information about all known OSPF neighbors.
details: Displays detailed information about all known OSPF neighbors.

---

route [summary]

Displays the OSPF routing table.
summary: Displays the number of intra-area, inter-area, external-1 and external-2 routes.

---

virtual-links

Displays the OSPF virtual links.

Usage

Use this command to display OSPF information.

Example

To display general OSPF information, enter the following command;

```
show ip ospf
```

show ip policy-forward

Displays information for IP packet redirecting policy for Home Agent (HA).

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show ip policy-forward
```

Usage

Use this command to see all the settings for IP packet redirection configuration from existing HA to new HA during upgrade.

Important: This is a customer specific command.

Example

The following command displays forward policy configuration for an HA:

```
show ip policy-forward
```

show ip pool

Displays statistics specific to IP pools.

Product

PDSN, GGSN, HA, ASN-GW, A-BG

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ip pool [address { pool-name *pool_name* **\| group-name** *group_name* **} { used \| free \| hold \| release } [limit** *limit* **] \| group-name** *group_name* **\| groups \| hold-timer { imsi** *imsi* **\| msid** *msid* **\| username** *username* **[imsi** *imsi* **\| msid** *msid* **] } \| overlap \| pool-name** *pool_name* **\| private \| public \| resource \| static \| summary \| verbose \| wide]**

address { pool-name *pool_name* **\| group-name** *group_name* **} { used \| free \| hold \| release} [limit** *limit* **]**

Displays IP pool addresses for the specified IP pool or pool group that are currently in the specified state.
pool-name *pool_name*: Displays IP addresses from an existing IP pool name specified as an alphanumeric string of 1 through 31 characters.
group-name *group_name*: Displays IP addresses from an existing IP pool group name specified as an alphanumeric string of 1 through 31 characters.
used: Displays the IP addresses that are in a used state.
free: Displays the IP addresses that are in a free state.
hold: Displays the IP addresses that are in a hold state.
release: Displays the IP addresses that are in a release state.
limit *limit*: Specifies the maximum number of address to display as an integer from 1 through 524287.

group-name *group_name*

Displays information about an existing IP pool group name specified as an alphanumeric string of 1 through 31 characters.

groups

Lists information about all IP pool groups.

hold-timer {imsi *imsi* **\| msid** *msid* **\| username** *username* **[imsi** *imsi* **\| msid** *msid*]}

Displays hold timer address information for the specified IMSI, MSID, or username.
imsi *imsi*: Displays hold-timer information for a valid IMSI (International Mobile Subscriber Identity), specified as a 15-character field that identifies the subscriber's home country and carrier.
msid *msid*: Displays hold-timer information for the MSID specified as a number from 7 through 16 digits.
username *username*: Displays hold-timer information for an existing username specified as an alphanumeric string of 1 through 127 characters.

Important: Active users cannot be displayed. If an active ID or username is entered, the following error message appears: Failure: No address matching the specified information was found! Please confirm that the options used match the network architecture/deployment,i.e. IMSI/MSID only, Username only, or IMSI/MSID plus Username. Please note that this command does not apply for addresses in the used state.

overlap

Lists information on overlapping IP pools

pool-name *pool_name*

Displays information about an existing IP pool.

private

Displays information about IP pools marked Private.

public

Displays information about IP pools marked Public.

resource

Displays information about resource IP pools.

static

Displays information about static IP pools.

summary

Displays a summary of all IP pool information.

verbose

Displays detailed information about all IP pools.

wide

Displays detailed information formatted to more than 80 columns.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display statistics pertaining to IP Pools in the current context.

Example

The following command displays IP address information for an IP Pool named *pool1*:

```
show ip pool address pool-name pool
```

To display a summary list for all IP pools in the current context, enter the following command:

```
show ip pool summary
```

The following command displays IP pool information for all IP pools configured in the current context:

show ip pool verbose

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ip ipsp

Displays the names of IP pools that are enabled for the IP pool sharing protocol (IPSP) and lists the disposition of addresses in the pools.

Product

PDSN, HA, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show ip ipsp [ summary ]
```

summary

Displays only the disposition of the addresses in the participating IP pools. Does not show the names of the participating IP pools.

Usage

Use this command to list the names of IP pools that are participating in the IPSP and list the disposition of IP addresses in those pools.

Important: For information on configuring and using IPSP refer to the *System Administration Guide*.

Example

To list information on all IPSP participating pools and address disposition, enter the following command:

```
show ip ipsp
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ip traffic sctp

Displays statistics that track Stream Control Transmission Control (SCTP) packets. This command obtains kernel SCTP traffic information for the specified card and CPU in a particular context.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ip traffic sctp card *<slot_number>* **cpu** *<cpu_number>*

card *<slot_number>*

Displays SCTP traffic for the card in slot number 1, 2, 8 or 9.

cpu *<cpu_number>*

Displays SCTP traffic for CPU number 0, 1, 2 or 3 on the specified card.

Usage

Use this command to debug the flow of SCTP traffic to a CPU kernel.

Example

To display SCTP traffic statistics for CPU 0 on the SMC in slot 8 enter the following command:

```
show ip traffic sctp card 8 cpu 0
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ipms status

Displays the status of Intelligent Packet Monitoring System (IPMS) client service with information related to system and call events. It also displays the status of configured IPMS servers.

Product

IPMS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ipms status [summary | all | server address *ip_address* **]**

summary

Displays the summary of all configured IPMS client and IPMS servers.

all

Displays information for all configured IPMS client and IPMS servers.

server address *ip_address*

Displays status for the IPMS server specified as an IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

This command is used to show/verify the status or configuration of one or all IPMS server along with system and call event information.

Example

The following command displays status of an IPMS server with IP address *10.2.3.4*:

```
show ipms status server address 10.2.3.4
```

show ipsg

Displays information and statistics specific to the IP Services Gateway (IPSG) service.

Product

IPSG

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ipsg { service { all [counters] | name *name* **} | sessions { all | callid** *num* **| counters {** *criteria* **} | full {** *criteria* **} | ip-address** *address* **| msid** *num* **| peer-address** *address* **| summary {** *criteria* **} | username** *name* **} | statistics [name** *name* **| peer-address** *address* **] } [| { grep** *grep_options* **| more }]**

---

service { all [counters] | name *name* **}**

Displays information about the configured IPSG service.
all [counters]: Displays information about all of the configured IPSG services on the system.
name *name*: Displays information about an existing IPSG service specified as an alphanumeric string of 1 through 63 characters.

---

sessions { all | callid *num* **| counters {** *criteria* **} | full {** *criteria* **} | imsi** *num* **| ip-address** *address* **| msid** *num* **| peer-address** *address* **| summary {** *criteria* **} | username** *name* **}**

all: Displays session information including call ID, NAI, and home address for all current IPSG sessions. This is the default behavior for the **sessions** keyword.
callid *num*: Displays session information for a current IPSG session based on the call ID specified as an 8-digit hexadecimal number.
counters { *criteria* }: Displays session counters for sessions matching the criteria. (See *criteria* below.)
full { *criteria* }: Displays all available session information for sessions matching the criteria. (See *criteria* below.)
ip-address *address*:
msid *num*: Displays session information for a current IPSG session based on the MSID. *num* must be an existing IPSG service session MSID, expressed as an 8-digit hexadecimal number.
peer-address *address*: Displays session information for a current IPSG session based on the IP address of the device sending the RADIUS accounting messages. *address* must be an existing IPSG service session IP address for the device sending the RADIUS accounting messages, entered using IPv4 dotted-decimal notation.
summary { *criteria* }: Displays a summary of available session information for sessions matching the criteria. (See *criteria* below.)
username *name*: Displays session information for a IPSG session based on the username of the subscriber specified as an alphanumeric string of 1 through 127 characters.
criteria:
all: Displays session information for all existing IPSG service sessions.
callid *num*: Displays session information for a specific IPSG session based on the call ID specified as an 8-digit hexadecimal number.
ip-address *address*: Displays session information for a specific IPSG session based on the IP address of the subscriber specified in IPv4 dotted-decimal notation.

msid *num*: Displays session information for an IPSG session based on the MSID.
peer-address *address*: Displays session information for a current IPSG session based on the IP address of the device sending the RADIUS accounting messages. *address* must be an existing IPSG service session IP address for the device sending the RADIUS accounting messages, entered using IPv4 dotted-decimal notation.
username *name*: Displays session information for a specific IPSG session based on the username of the subscriber. *name* is an existing IPSG service session subscriber username, expressed as an alphanumeric string of 1 through 127 characters.

statistics [name *name* **| peer-address** *address* **]**

Displays the total collected statistics of all IPSG sessions since the last system restart or clear command.
name *name*: Displays the total collected statistics of all IPSG sessions processed by a specific service since the last system restart or clear command. *name* must be an existing IPSG service name expressed as an alphanumeric string of 1 through 63 characters.
peer-address *address*: Displays the total collected statistics of all IPSG sessions associated with a specific IP address of the device responsible for sending the RADIUS accounting messages. Displayed statistics are from the last system restart or clear command.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information and statistics about existing IPSG services.

Example

The following command displays the existing IPSG services on the system:

```
show ipsg service all
```

The following command displays all the existing IPSG service sessions on the system:

```
show ipsg session all
```

The following command displays the cumulative IPSG session statistics on the system:

```
show ipsg statistics
```

The following command displays the cumulative IPSG session statistics on the system for an IPSG service named *ipsg1*:

```
show ipsg statistics name ipsg1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ipv6

Displays information for each rule in an IPv6 access control group.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ipv6 { **access-group** [**statistics**] [**|** { **grep** *grep_options* | **more** }] | **access-list** [*list_name*] [**|** { **grep** *grep_options* | **more** }] | **interface** [**name** *interface_name* [**statistics**] | **summary** | **vrf** *vrf_name* | **|** { **grep** *grep_options* | **more** }] | **neighbors** [*IPv6-ADDRESS*] [**vrf** *vrf_name*] | [**|** { **grep** *grep_options* | **more** }] }

access-group

Displays all configured access groups in the current context along with the priority values.

statistics

Displays statistics for each rule in an IPv6 access control group.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

access-list [*list_name* **]**

Displays IPv6 access control list information an existing access list name specified as an alphanumeric string of 1 through 47 characters.

interface

Displays interface information for the current context.

name *interface_name*

Displays detailed information for an existing interface name specified as an alphameric string of 1 through 79 characters.

statistics

Displays the number of inbound and outbound IP packets registered by kernel.

summary

Displays summary information about all IP interfaces.

vrf *vrf_name*

Displays information related to an existing VRF specified as an alphanumeric string of 1 through 63 characters.

neighbors [*ipv6_address* **]**

the IP address specified in IPv6 colon-separated notation.

Usage

Show the IPv6 information to verify and/or troubleshoot communication between/to a remote host/node.

Example

The following command displays the ACL for the list named *sampleACL*.

```
show ipv6 access-list sampleACL samplev6ACL
```

The following command displays the interface information, including statistics, for the IPv6 interface *samplev6interface*.

```
show ipv6 interface name samplev6interface statistics
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ipv6 ospf

Displays information regarding the configuration of the OSPFv3 Protocol on this system.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ipv6 ospf [database | debugging | interface | nieghbor | route | virtual-links] [verbose [verbose] [| { grep *grep_options* **| more }]**

show ipv6 ospf database [adv-router*ipv4-address* **] [ls-type { external | inter-prefix | inter-router | intra-prefix | link | network | router }**

show ipv6 ospf debugging

show ipv6 ospf interface

show ipv6 ospf neighbor [details]

show ipv6 ospf route [summary]

show ipv6 ospf virtual-links

---

show ipv6 ospf database

Displays the OSPFv3 database including the following components.

- **adv-router** *ipv4-address*: Displays OSPF database information from the advertising router specified as an IP address in IPv4 dotted-decimal notation.
- **ls-type**: Displays the specified Link-State Advertisement (LSA) type, which can be one of the following:
  - **external**: Display External LSA information
  - **inter-prefix**: Displays Inter Area Prefix LSA information
  - **inter-router**: Displays Inter Area Router LSA information
  - **intra-prefix**: Displays Intra Area Prefix LSA information
  - **link**: Displays Link LSA information
  - **network**: Displays Network LSA information
  - **router**: Displays Router LSA information

---

show ipv6 ospf debugging

Displays OSPFv3 Debugging Flags.

---

show ipv6 ospf interface

Displays OSPFv3 Interfaces.

show ipv6 ospf neighbor [details]

Displays OSPFv3 neighbors with the option for full details.

show ipv6 ospf route [summary]

Displays OSPFv3 route information with the option for summarized information.

show ipv6 ospf virtual-links

Displays OSPFv3 virtual links.

verbose

Displays detailed information.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to see all OSPFv3 information.

Example

The following command displays ipv6 ospf information:

```
show ipv6 ospf
```

show ipv6 pool

Displays information related IPv6 Pool configuration/state.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ipv6 pool[**group-name***group-name*] [**pool-name***pool-name*] [**summary**] [**verbose**] [**|** { **grep** *grep_options* | **more** }]

group-name*group-name*

Displays IP address pool information for an existing group-name specified as an alphanumeric string of 1 through 31 characters.

pool-name *pool-name*

Displays IPv6 address pool information for an existing pool name specified as an alphanumeric string of 1 through 31 characters.

summary

Displays summary information about all IP address pools; this is the default.

verbose

Displays detailed information about all IP address pools.

| { grep *grep_options*|**more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to see all the ipv6 pool information.

Example

The following command displays ipv6 pool information:

```
show ipv6 pool
```

show ipv6 prefix-list

Displays information related to an IPv6 prefix list.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ipv6 prefix-list[**detail***prefix-list-name*] [**name***prefix-list-name* [*ip-address/mask* [**longer**] [**match-first**]] [**seq** *seq_value*]] [**summary** *prefix-list-name*] [**|** { **grep** *grep_options* | **more** }]

detail*prefix-list-name*

Displays detailed IP address information for an existing prefix-list specified as an alphanumeric string of 1 through 79 characters.

name*prefix-list-name*

Displays IP address information for an existing prefix-list specified as an alphanumeric string of 1 through 79 characters.

ip-address/mask

Specifies an IPv6 Network Address/Mask Bits combination in CIDR notation.

longer

Displays IP address prefix-list details in longer format.

match-first

Displays first matched IP address prefix-list details.

seq *seq_value*

Specifies the sequence number as an integer from 1 through 4294967295.

seq_value is the integer value between 1 through 4294967295.

summary *prefix-list-name*

Displays prefix-list summary for an existing prefix-list specified as an alphanumeric string of 1 through 79 characters.

| { grep *grep_options*|**more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to see all the ipv6 prefix-list information.

Example

The following command displays ipv6 prefix-list information:

```
show ipv6 prefix-list
```

show ipv6 route

Displays information related to specific route for current context.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ipv6 route [*ip-address/mask*] [**vrf** *vrf-name*] [**|** { **grep** *grep_options* | **more** }]

ip-address/mask

Specifies an IP address entered using IPv6 colon-separated and CIDR notation.

vrf *vrf-name*

Displays Virtual Routing and Forwarding (VRF) routing information for an existing VRF specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options*|**more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to see all the ipv6 route information.

Example

The following command displays ipv6 route information:

```
show ipv6 route 2001:0db8:85a3:0000:0000:8a2e:0370:7334/5
```

show ipv6 route-access-list

Displays the route access list.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ipv6 route-access-list [*route-access-list*] [**|** { **grep** *grep_options* | **more** }]

route-access-list

route-access-list is an alphanumeric string of 1 through 79 characters.

| { grep *grep_options*|**more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to see all the IPv6 route access list information.

Example

The following command displays ipv6 route access list information:

```
show ipv6 route-access-list
```

show iups-service

Displays information for Iu-PS services in the current context. The IuPS interface links the Radio Network Controller (RNC) with the Packet Switched Core Network.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show iups-service { all | name *srvc_name***} [gtpu-table | rnc { all | id** *rnc_id* **}] [| { grep** *grep_options* **| more }]**

all

Shows information for all configured IuPS services.

name *srvc_name*

Specifies an existing IuPS service as an alphanumeric string of 1 through 63 characters.

gtpu-table

Displays the configured GTPU database.

rnc all

Displays information for all configured RNCs.

rnc *rnc_id*

Specifies the identification number of an existing RNC configuration instance as an integer from 0 through 4095.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Iu-PS services control the interface between the SGSN and the RNCs in the UMTS radio access network (UTRAN). Iu-PS services include the control plane and the data plane between these nodes.
Use this command to display information for a specific Iu-PS service or for all Iu-PS services configured within the context. A filtering keyword can limit the display to only information for a specific RNC or for a GTPU table in the Iu-PS service configuration.

Example

The next command displays information for all Iu-PS services configured in the current context:

```
show iups-service all
```

This command displays information for a specific RNC for a specific Iu-PS services:

```
show iups-service name iups-svc-1 rnc 123name
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show l2tp sessions

Displays information for Layer 2 Tunneling Protocol (L2TP) tunnels.

Product

LNS, PDSN, GGSN, HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show l2tp sessions [full | summary | counters] [all | callid *id* **| username** *name* **| msid** *ms_id* **| lac-service** *service_name* **| lns-service** *service_name* **peer-address [** *operator* **]** *peer_address* **]**

full

Displays all available information for the specified sessions.

summary

Displays a summary of available information for the specified sessions.

counters

Displays counters for the specified L2TP sessions.

all

Displays all current sessions.

callid *id*

Displays session information for the call ID. specified an 8-byte hexadecimal number. The output of the command **show l2tp tunnels** contains a field labeled Callid Hint which lists the call ID information to use with this command.

username *name*

Displays session information for an existing subscriber specified as an alphanumeric string of 1 through 127 characters. Wildcard characters $ and * are allowed.

msid *ms_id*

Displays session information for the MSID specified as 7 to 16 digits for an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed.

lac-service *service_name*

Displays all L2TP sessions in the specified LAC service.

lns-service *service_name*

Displays all L2TP sessions in the specified LNS service.

peer-address [*operator* **]** *peer_address*

Displays all L2TP sessions to the destination (peer LNS) specified as an IP address in IPv4 dotted-decimal notation.
In conjunction with **sessions** keyword, indicates a range of peers is to be displayed.
peer-address [*operator*] *peer_address* is specified using IPv4 dotted-decimal notation.
operator implies how to logically specify a range of peer-address and it must be one of the following:

- **<**: IP address less than the specified *peer_address*
- **>**: IP address less than the specified *peer_address*
- **greater-than**: IP address less than the specified *peer_address*
- **less-than**: IP address less than the specified *peer_address*

Usage

Use this command to show information for sessions in the current context.

Important: If this command is executed from within the local context, cumulative session information is displayed for all contexts.

Example

The following command displays cumulative statistics for all sessions processed within the current context:

```
show l2tp sessions
```

The following command displays all information pertaining to the L2TP session of a subscriber named *isp1vpnuser1*:

```
show l2tp session full username isp1vpnuser1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show l2tp statistics

Displays statistics for all Layer 2 Tunneling Protocol (L2TP) tunnels and sessions.

Product

LNS, PDSN, GGSN, HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show l2tp statistics [lac-service *service_name* **| lns-service** *service_name* **| peer-address** *peer_ip_address* **]**

lac-service *service_name*

Displays L2TP statistics for all tunnels and sessions in an existing L2TP Access Concentrator (LAC) service specified as an alphanumeric string of 1 through 63 characters.

lns-service *service_name*

Displays L2TP statistics for all tunnels and sessions in tan existing L2TP Network Server (LNS) service specified as an alphanumeric string of 1 through 63 characters.

peer-address *peer_address*

Displays L2TP statistics for all tunnels and sessions to the destination (peer LNS) at the IP address specified in IPv4 dotted-decimal notation.

Usage

Use this command to display statistics for L2TP services.

Example

The following command displays statistics for a specific LAC service named *vpn1*:

```
show l2tp statistics lac-service vpn1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show l2tp tunnels

Displays information for Layer 2 Tunneling Protocol (L2TP) tunnels.

Product

LNS, PDSN, GGSN, HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show l2tp tunnels [full | summary | counters] [all | callid *id* **| username** *name* **| msid** *ms_id* **| lac-service** *service_name* **| lns-service** *service_name* **| peer-address [** *operator* **]** *peer_address* **]**

full

Displays all available information for the specified tunnels.

summary

Displays a summary of available information for the specified tunnels.

counters

Displays counters for the specified L2TP tunnels.

all

Displays all current tunnels.

callid *id*

Displays tunnel information for the call id specified as an 8-digit hexadecimal number. The output of the command **show l2tp tunnels** contains a field labeled Callid Hint which lists the call id information to use with this command.

username *name*

Displays tunnel information for an existing subscriber specified as an alphanumeric string of 1 through 127 characters. Wildcard characters $ and * are allowed.

msid *ms_id*

Displays tunnel information for the MSID specified as 7 to 16 digits for an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed.

lac-service *service_name*

Displays all L2TP tunnels in the specified LAC service.

lns-service *service_name*

Displays all L2TP tunnels in the specified LNS service.

peer-address [*operator* **]** *peer_address*

Displays all L2TP tunnels to the destination (peer LNS) at the IP address specified in IPv4 dotted-decimal notation.
In conjunction with **tunnels** keyword, indicates a range of peers is to be displayed.
peer-address [*operator*]: Specifies a peer address using IPv4 dotted-decimal notation.
operator implies how to logically specify a range of peer-address and it must be one of the following:

- **<**: IP address less than the specified *peer_address*
- **>**: IP address less than the specified *peer_address*
- **greater-than**: IP address less than the specified *peer_address*
- **less-than**: IP address less than the specified *peer_address*

Usage

Use this command to show information for tunnels in the current context.

Example

The following command displays all of the tunnels currently being facilitated by LAC services within the current context:

```
show l2tp tunnels all
```

The following command displays information pertaining to the L2TP tunnel(s) established for a LAC-service named vpn1:

```
show l2tp tunnels full lac-service vpn1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a full description of this command.

show lawful-intercept ssdf statistics

Refer to the *Lawful Intercept Configuration Guide* for a description of these statistics.

show lac-service

Displays the information for all L2TP Access Concentrator (LAC) services or for a particular LAC service.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show lac-service { all | name *service_name* **} [| { grep** *grep_options* **| more }]**

all

Display information for all LAC services.

name *service_name*

Display information only for an existing LAC service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to list information for LAC services configured on this system.

Example

The following commands display information for all LAC services and the LAC service named *lac1*, respectively.

```
show lac-service allshow lac-service name lac1
```

show leds

Displays the current status of the light emitting diodes (LEDs) for a specific card or all cards.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show leds { all | *card_num* } [| { grep *grep_options* | more }]

all | *card_num*

all: Displays the LED status for all cards.
card_num: Displays the LED status for the card specified by its slot number.

| { grep *grep_options* | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Display the status of the LEDs as a part of an automated periodic script which checks the LEDs of the chassis.

Important: This command is not supported on all platforms.

Example

The following commands display the LED status for all cards and only card *8*, respectively.

```
show leds all

show leds 8
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show license information

Displays information about the licenses installed on this system, as well as the maximum number of sessions.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show license information { *key_name* | full } | { key } [| { grep *grep_options* | more }]

***key_name* | full**

key_name: Displays the information for an existing license key specified as an alphanumeric string of 1 of 1 through 500 characters.
full: Displays the full features and quantities without any hardware limits in place.

key:

Displays the installed keys in encrypted format.

| { grep *grep_options* | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Displays the license information to verify the proper keys have been installed. This command is also helpful in troubleshooting user system access due to the maximum number of sessions being reached.

Example

The following displays the encrypted installed key and the information for *sampleKey* respectively.

```
show license information sampleKey
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show linecard

Displays information on the interface cards installed in the rear of the system chassis.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show linecard { dlci-utilization *card#* **| table } [| { grep** *grep_options* **| more }]**

dlci-utilization *card#*

SGSN only
In tabular format, displays current data link utilization (in 5 minute and 15 minute breakdowns) information for all Frame Relay ports on the specified CLC-type line card. Data links are referred to by data link connection identifiers (DLCI).
card# - Identifies the chassis slot number where the line card resides. Enter an integer from 1 to 48.

table

Displays information on all line card slots in tabular format.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to show the line card information

- to verify hardware inventories and installed components.
- to review DLCI utilization for a specific Frame Relay channelized line card.

Important: This command is not supported on all platforms.

Example

Use the following command to display a table with information identifying all line cards installed in the chassis:

```
show linecard table
```

Use the following command to display DLCI utilization information for all ports on CLC card in slot 27:

```
show linecard dlci-utilization 27
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show linkmgr

Displays statistics for the link manager (linkmgr).

Product

SGSN

Privilege

Inspector

Syntax

show linkmgr { all | instance *instance* **} [parser | |]**

all

Display statistics for all link managers.

instance *instance*

Display statistics for a single instance of a link manager specified as an integer from 1 to 4.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

This command displays statistical information for the SGSN's link manager which handles the layer between the session manager and the SS7 functionality downwards from layer 3.

Example

Use the following command to display the statistics for link manager *4*:

```
show linkmgr 4
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show llc statistics

Displays traffic statistics for the GPRS logical link-control (LLC) layer.

Product

SGSN

Privilege

Inspector

Syntax

show llc statistics [gprs-service *srvc_name* **] [verbose] [| { grep grep_options | more }]**

gprs-service *srvc_name*

Displays the statistics for an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

verbose

Displays all possible statistics for specified command or keyword.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference*.

Usage

This command can display either a summarized or full (verbose) view of statistics collected for the traffic that has gone through the LLC layer for either all GPRS services or for a specified GPRS service.

Example

The following command displays the frame Tx/Rx LLC statistics for GPRS service *gprs1*:

```
show llc statistics gprs-service gprs1
```

show llc status

Displays status information for the GPRS logical link-control (LLC) layer.

Product

SGSN

Privilege

Inspector

Syntax

show llc status gprs-service *srvc_name* **sessmgr instance** *instance* **{ dlci ms-id** *ms_id* **sapi** *sapid* **| lsap sapid** *sapid* **| ms** *ms_id* **| usap sapid** *sapid* **[| { grep grep_options | more }]**

---

gprs-service *srvc_name*

Displays the LLC layer status for an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

---

sessmgr instance *instance*

Displays the LLC status for a session manager instance specified as an integer from 1 to 4294967295.

---

dlci ms-id *ms_id* **[sapi** *sapid* **]**

Displays the LLC status for a specific data link connection identifier (DLCI) between the LLC and the mobile station (MS). *ms_id* must be an integer from 0 to 65536 that identifies the DLCI interface connecting to a specific MS.
sapi: Filters the display of the LLC status information to focus on a specific service access point interface (SAPI) within the specified DLCI specified as.an integer from 1 to 11

---

lsap *sapid*

Refines the display of the LLC status to focus on a specific lower service access point interface (LSAP) specified as an integer from 0 to 65536.

---

ms-id *ms_id*

Displays the LLC status for a connected MS specified as an integer from 0 to 65536.

---

usap *sapid*

Refines the display of the LLC statistics to focus on a specific upper service access point interface (USAP) specified as an integer from 0 to 65536.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference*.

Usage

This command can display either a summarized or full (verbose) view of statistics collected for the traffic that has gone through the LLC layer for either all GPRS services or for a specified GPRS service.

Example

The following command displays the frame Tx/Rx LLC statistics for GPRS service *gprs1*:

```
show llc statistics gprs-service gprs1
```

show lma-service

Displays statistic and counter information for Local Mobility Anchor (LMA) services on this system.

Product

P-GW

Privilege

Inspector

Syntax

show lma-service all

show lma-service name *service_name*

show lma-service session [all | callid *id* **| counters | full | ipv6-address { <** *address* **| >** *address* **|** *address* **| greater-than** *address* **[less-than** *address* **] | less-than** *address* **[greater-than** *address* **] } | summary | username** *name* **]**

show lma-service statistics [lma-service *name* **] } [| { grep** *grep_options* **| more }]**

---

all

Displays information about all configured LMA services on this system.

---

name *service_name*

Displays configuration information for an existing LMA service specified as an alphanumeric string of 1 through 63 characters.

---

session [all | callid *id* **| counters | full | ipv6-address { <** *address* **| >** *address* **|** *address* **| greater-than** *address* **[less-than** *address* **] | less-than** *address* **[greater-than** *address* **] } | summary | username** *name* **]**

Displays session information filtered by the following parameters:
all: Displays all active LMA sessions using LMA services on the system.
callid *id*: Displays available session information for the call identification number specified as an eight-byte hexadecimal number.
counters: Displays session counters for active LMA sessions using LMA services on the system. This keyword can also be filtered by the following:

- **all**
- **callid**
- **ipv6-address**
- **username**

Refer to the keyword descriptions in this command for information regarding these filters.
full: Displays additional session information for active LMA sessions using LMA services on the system. This keyword includes the information in the output of the **all** keyword plus additional information. This keyword can also be filtered by the following:

- **all**
- **callid**
- **ipv6-address**

- **username**

Refer to the keyword descriptions in this command for information regarding these filters.

ipv6-address:

- **<** *address* and **less-than** *address*: Displays summarized information for a group of IPv6 addresses that are less than the specified IPv6 address using one of these keywords. A range can be specified by including an address with the **greater-than** option. *address* must be specified in IPv6 colon-separated notation.
- **>** *address* and **greater-than** *address*: Displays summarized information for a group of IPv6 addresses that are greater than the specified IPv6 address using one of these keywords. A range can be specified by including an address with the **less-than** option. *address* must be specified in IPv6 colon-separated notation.
- *address*: Displays summarized information for a specific IPv6 address using an LMA service on this system. *address* must be specified in IPv6 colon-separated notation.

summary: Displays the number of LMA sessions currently active for LMA services configured on the system.

username *name*: Displays available session information for an existing user specified as an alphanumeric string of 1 through 127 characters.

---

statistics [lma-service *name* **]**

lma-service *name*: Displays LMA service statistics for an existing LMA service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of Chapter 1 of the *Command Line Interface Reference Guide*.

Usage

Use this command to view configuration information for LMA services on this system.

Example

The following command displays service statistics for the LMA service named *lma1*:

```
show lma-service name lma1
```

show lns-service

Displays the information for all L2TP Network Server (LNS) services or for a particular LNS service.

Product

PDSN, HA, GGSN, LNS

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show lns-service { all | name *service_name* **} [| { grep** *grep_options* **| more }]**

all

Display information for all LNS services.

name *service_name*

Displays information only for an existing LNS service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to list information for LNS services configured on this system.

Example

The following commands display information for all LNS services and the LNS service named *lns1*, respectively.

```
show lns-service all

show lns-service name lns1
```

show local-user

Displays information pertaining to local-user accounts.

Product

All

Privilege

Security Administrator

Syntax

show local-user [[username *name* **] [inactive** *filter* **] [verbose | wide] | statistics [verbose]]**

username *name*

Displays information for an existing local-user administrative account specified as an alphanumeric string of 3 through 16 characters that is case sensitive.

inactive *filter*

Specifies a filter for displaying inactive local-user accounts:

- **<** *days*: Displays accounts that have been inactive less than the specified number of days.
- **>** *days*: Displays accounts that have been inactive more than the specified number of days.
- **greater-than** *days*: Displays accounts that have been inactive more than the specified number of days.
- **less-than** *days*: Displays accounts that have been inactive less than the specified number of days.

days can be configured to an integer from 1 through 365.

[verbose | wide]

Specifies how the information is to be displayed as one of the following options:

- **verbose**: The data is displayed in list format. Additional information is provided beyond what is displayed when the **wide** option is used.
- **wide**: The data is displayed in tabular format. This is the default setting.

statistics [verbose]

Displays local-user statistics.
Using the **verbose** keyword displays additional statistics.

Usage

Use this command to display information and statistics on local-user administrative accounts.

Example

The following command displays detailed information on local-user administrative accounts that have been inactive for more than 10 days:

```
show local-user inactive greater-than 10 verbose
```

The following command displays detailed information for a local-user account named *Test*:

```
show local-user username Test verbose
```

The following command displays detailed local-user account statistics:

```
show local-user statistics verbose
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show logging

Displays the defined logging filters for the current context.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show logging [active | verbose] [| { grep *grep_options* **| more }]**

active | verbose

active: Displays only active CLI logging filter information in concise format.
verbose: Displays as much information as possible.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View log filters to troubleshoot disk utilization issues.

Example

```
show logging

show logging active

show logging verbose

show logging active verbose
```

show logs

Displays active and inactive logs filtered by the options specified.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show logs [active] [inactive] [callid *call_id* **] [event-verbosity** *evt_verboseness* **] [facility** *facility* **] [level** *severity_level* **] [pdu-data** *pdu_format* **] [pdu-verbosity** *pdu_verboseness* **] [proclet** *facility* **] [since** *from_date_time* **[until** *to_date_time* **]] [| { grep** *grep_options* **| more }]**

active

Displays data from active logs.

inactive

Displays data from inactive logs.

callid *call_id*

Displays log information only for a call ID specified as a 4-digit hexadecimal number.

event-verbosity *evt_verboseness*

Specifies the level of verboseness to use in displaying of event data as one of:

- **min** - displays minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.
- **concise** - displays detailed information about the event, but does not provide the event source within the system.
- **full** - displays detailed information about event, including source information, identifying where within the system the event was generated.

facility *facility*

Specifies the facility to modify the filtering of logged information for as one of:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: AAA client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **aal2**: AAL2 protocol logging facility
- **acl-log**: Access Control List logging facility

- **acsctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: Active Charging Service (ACS) Manager facility
- **alarmctrl**: Alarm Controller facility
- **alcap**: ALCAP protocol logging facility
- **alcapmgr**: ALCAPMgr logging facility
- **all**: All facilities
- **asngwmgr**: ASN Gateway Manager facility
- **asnpcmgr**: ASN Paging Controller Manager facility
- **bfd**: BFD protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux-De-mux Manager logging facility
- **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
- **callhome**: Call home application logging facility
- **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
- **cli**: CLI logging facility
- **credit-control**: Credit Control facility
- **cscf**: IMS/MMD CSCF
- **cscfmgr**: SIP CSCF Manager facility
- **cscfttmgr**: SIP CSCFTT Manager facility
- **csp**: Card Slot Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: Content Service Selection (CSS) RADIUS Signaling facility
- **cx-diameter**: Cx Diameter Messages facility
- **dcardctrl**: IPSEC Daughter Card Controller logging facility
- **dcardmgr**: IPSEC Daughter Card Manager logging facility
- **demuxmgr**: Demux Manager API facility
- **dgmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol logging facility
- **dhcpv6**: DHCPv6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages facility
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting
- **diameter-auth**: Diameter Authentication

- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ACS Diameter signaling facility
- **diameter-hdd**: Diameter HDD Interface facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSEC Data Path facility
- **drvctrl**: Driver Controller facility
- **eap-ipsec**: EAP
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface facility
- **egtpc**: eGTP-C logging facility
- **egtpmgr**: eGTP manager logging facility
- **egtpu**: eGTP-U logging facility
- **epdg**: ePDG logging facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
- **fng**: FNG logging facility
- **gmm**:
    - For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
    - For 3G: Logs the access application layer (above the RANAP layer)
- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
- **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
- **gss-gcdr**: GTPP Storage Server GCDR facility
- **gtpc**: GTP-C protocol logging facility
- **gtpcmgr**: GTP-C protocol Manager logging facility
- **gtpp**: GTP-PRIME protocol logging facility
- **gtpu**: GTP-U protocol logging facility
- **gtpumgr**: GTPU Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages facility
- **gy-diameter**: Gy Diameter messages facility
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **hdctrl**: HD Controller logging facility
- **hnb-gw**: HNB-GW (3G Femto GW) logging facility
- **hnbmgr**: HNBMGR (3G Femto GW DemuxMgr) logging facility

- **hss-peer-service**: HSS Peer Service facility
- **igmp**: IGMP
- **ikev2**: IKEv2
- **ims-authorizatn**: IMS Authorization Service facility
- **ims-sh**: HSS SH Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **imsue**: IMSUE
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipms**: IPMS logging facility
- **ipsec**: IP Security logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ipsp**: IP Pool Sharing Protocol logging facility
- **kvstore**: KV Store facility
- **l2tp-control**: L2TP control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: LAGMGR logging facility
- **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
- **li**: Refer to the *Lawful Intercept Interface Reference* for a description of this command.
- **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
- **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
- **local-policy**: Local Policy Service facility
- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway manager logging facility
- **map**: MAP Protocol logging facility
- **megadiammgr**: Megadiameter Manager (SLF Service) logging facility
- **mme-app**: Mobility Management Entity Application logging facility
- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: Mobility Management Entity Demux Manager logging facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes

- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 logging facility
- **mpls**: MPLS protocol logging facility
- **mseg-app**: MSEG application logging facility
- **mseg-gtpc**: MSEG GTPC application logging facility
- **mseg-gtpu**: MSEG GTPU application logging facility
- **msegmgr**: MSEGMgr (MSEG DemuxMgr) logging facility
- **mtp2**: MTP2 Service logging facility
- **mtp3**: MTP3 Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **npuctrl**: Network Processor Unit Control facility
- **npumgr**: Network Processor Unit Manager facility
- **npumgr-acl**: NPUMGR ACL logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility
- **npumgr-fwd**: NPUMGR FWD logging facility
- **npumgr-init**: NPUMGR INIT logging facility
- **npumgr-port**: NPUMGR PORT logging facility
- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **ntfy-intf**: Notification Interface logging facility
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF protocol logging facility
- **ospfv3**: OSPFv3 protocol logging facility
- **p2p**: Peer-to-Peer Detection logging facility
- **pccmgr**: IPCF PCC Manager library
- **pdg**: PDG logging facility
- **pdgdmgr**: PDG Demux Manager logging facility
- **pdif**: PDIF logging facility
- **pgw**: PDN Gateway logging facility
- **phs**: Payload Header Suppression
- **phs-control**: PHS X1/X5 and X2/X6 Interface logging facility
- **phs-data**: PHS Data logging facility
- **phs-eapol**: PHS EAPOL logging facility
- **phsgwmgr**: PHS Gateway Manager facility
- **phspcmgr**: PHS Paging Controller Manager facility
- **pmm-app**: PMM application logging facility
- **ppp**: PPP link and packet facilities
- **pppoe**: PPPOE logging facility

- **push**: VPNMGR CDR push logging facility
- **radius-acct**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Rf Diameter messages facility
- **rip**: RIP logging facility (RIP is not supported at this time.)
- **rohc**: RObust Header Compression facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RUA (3G Femto GW - RUA messages) logging facility
- **s1ap**: S1AP Protocol logging facility
- **sccp:** SCCP Protocol logging connection-oriented messages between RANAP and TCAP layers.
- **sct**: Shared Configuration Task logging facility
- **sctp**: SCTP Protocol logging facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN ‘glue’ interfaces, e.g., between PMM, MAP,. GPRS-FSM, SMS.
- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN MBMS Bearer app (SMGR) logging facility
- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSNs System Components logging facility; used infrequently
- **sgsn-test**: SGSN Tests logging facility; used infrequently
- **sgtpcmgr**: SGSN GTPC Manager logging information exchange through SGTPC and the GGSN
- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages facility
- **sitmain**: System Initialization Task main logging facility
- **sm-app**: SM Protocol logging facility

- **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
- **sndcp**: SNDCP Protocol logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF SPR Manager logging facility
- **srdb**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **sscfnni**: SSCFNNI Protocol logging facility
- **sscop**: SSCOP Protocol logging facility
- **ssh-ipsec**: SSH IP Security logging facility
- **ssl**: SSL (Secure socket layer messages) logging facility
- **stat**: Statistics logging facility
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **tcap**: TCAP Protocol logging facility
- **testctrl**: Test Controller logging facility
- **testmgr**: Test Manager logging facility
- **threshold**: threshold logging facility
- **ttg**: TTG logging facility
- **tucl**: TUCL logging facility
- **udr**: User detail record facility (used with the Charging Service)
- **user-data**: User data logging facility
- **user-l3tunnel**: User layer-3 tunnel logging facility
- **usertcp-stack**: User TCP Stack
- **vpn**: Virtual Private Network logging facility
- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6

---

level *severity_level*

level *severity_level*: Specifies the level of information to be logged from the following list which is ordered from highest to lowest:

- **critical** - display critical events
- **error** - display error events and all events with a higher severity level
- **warning** - display warning events and all events with a higher severity level
- **unusual** - display unusual events and all events with a higher severity level
- **info** - display info events and all events with a higher severity level
- **trace** - display trace events and all events with a higher severity level
- **debug** - display all events

pdu-data *pdu_format*

Specifies output format for the display of packet data units as one of:

- **none** - output is in raw format (unformatted).
- **hex** - output being displayed in hexadecimal format.
- **hex-ascii** - output being displayed in hexadecimal and ASCII similar to a main-frame dump.

pdu-verbosity *pdu_verboseness*

Specifies the level of verboseness to use in displaying of packet data units as an integer from 1 through 5, where 5 is the most detailed.

proclet *facility*

Shows the logs from a specific proclet facility. The available facilities are the same as those listed earlier.

since *from_date_time* **[until** *to_date_time* **]**

Default: no limit.
since *from_date_time*: indicates only the log information which has been collected more recently than *from_date_time* is to be displayed.
until *to_date_time*: indicates no log information more recent than *to_date_time* is to be displayed. **until** defaults to current time when omitted.
from_date_time and *to_date_time* must be formatted as YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where:

- YYYY = 4-digit year
- MM = 2-digit month in the range 01 through 12
- DD = 2-digit day in the range 01 through 31
- HH = 2-digit hour in the range 00 through 23
- mm = 2-digit minute in the range 00 through 59
- ss = 2-digit second in the range 00 through 59

to_date_time must be a time which is more recent than *from_date_time*.
The use of the **until** keyword allows for a time range of log information while only using the **since** keyword will display all information up to the current time.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View log files for general maintenance or troubleshooting system issues.

Example

The following command displays log information for the *a11mgr* facility starting with July 1th, 2011 at midnight.

```
show logs facility allmgr since 2011:07:11:00:00
```

The following command displays the log information for call ID *FE881D32* only in active logs.

```
show logs active callid FE881D32
```

show lte-policy

Displays information for Long term Evolution (LTE) policy configurations on this system including handover restriction lists, subscriber maps, and tracking area identifiers (TAIs).

Product

MME

Privilege

Inspector

Syntax

show lte-policy { ho-restriction-list { name *name* **| summary } | subscriber-map { name** *name* **| summary } | tai-mgmt-db { name** *name* **| summary } } [| { grep** *grep_options* **| more }]**

ho-restriction-list { name *name* **| summary }**

Displays information about handover restriction lists configured on this system.
name *name*: Displays information about a specific handover restriction list configured on this system. *name* must be an existing HO restriction list, expressed as an alphanumeric string of 1 to 64 characters.
summary: Displays summarized information about all handover restriction lists configured on this system.

subscriber-map { name *name* **| summary }**

Displays information about subscriber maps configured on this system.
name *name*: Displays information about an existing subscriber map specified as an alphanumeric string of 1 through 64 characters.
summary: Displays summarized information about all subscriber maps configured on this system.

tai-mgmt-db { name *name* **| summary }**

Displays information about TAI management databases configured on this system.
name *name*: Displays information about an existing TAI management database specified as an alphanumeric string of 1 through 64 characters.
summary: Displays summarized information about all TAI management databases configured on this system.

| { grep *grep_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *CLI Overview* chapter.

Usage

Use this command to display information for LTE policy configurations on this system including handover restriction lists, subscriber maps, and tracking area identifiers (TAIs).

Example

The following command displays information about a subscriber map named *map3*:

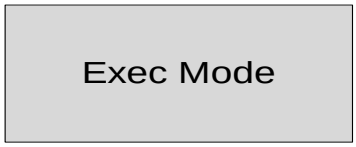
```
show lte-policy subscriber-map name map3
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

Chapter 117
Exec Mode Show Commands (M-P)

This section includes the commands **`show m3ua statistics`** through **`show profile-id-qci-mapping`**.

The Exec Mode is the initial entry point into the command line interface system. Exec mode **show** commands are useful in troubleshooting and basic system monitoring.



show mag-service

Displays statistic and counter information for Mobile Access Gateway (MAG) services on this system.

Product

HSGW, S-GW

Privilege

Inspector

Syntax

show mag-service { all | name *service_name* **| session [all | callid** *id* **| counters | full | ip-address** *home_ip_address* **| msid** *id* **| summary | username** *name* **] | statistics [name** *service_name* **] } [| { grep** *grep_options* **| more }]**

---

all

Displays information for all configured MAG services on this system.

---

name *service_name*

Displays configuration information for a specific MAG service configured on this system.
service_name must be an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

---

session [all | callid *id* **| counters | full | ip-address** *home_ip_address* **| msid** *id* **| summary | username** *name* **]**

all: Displays all active MAG sessions using MAG services on the system.
callid *id*: Displays available session information for the specific call identification number.
id must be an 8-digit hexadecimal number.
counters: Displays counters for all MAG services on the system.This keyword can also be filtered by the following:

- **all**
- **callid**
- **ip-address**
- **msid**
- **summary**
- **username**

Refer to the keyword descriptions in this command for information regarding these filters.
full: Displays additional session information for all active MAG sessions using MAG services on the system. This keyword includes the information in the output of the **all** keyword plus additional information. This keyword can also be filtered by the following:

- **all**
- **callid**
- **ip-address**
- **msid**
- **summary**

- **username**

Refer to the keyword descriptions in this command for information regarding these filters.
ip-address *home_ip_address*: Displays available session information for a specific home IPv4 or IPv6 address of a subscriber in a service session.
msid *id*: Displays available information for a specific mobile station identification number or group of numbers based on wildcard entry.
id must be a valid MSID number and can be a sequence of characters and/or wildcard characters ('$' and/or '*'). The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes (‘). For example: ‘$’.
summary: Displays the number of MAG sessions currently active for MAG services configured on the system.
username *name*: Displays available session information for a specific user in a service session.
name must be followed by an existing user name expressed as an alphanumeric string of 1 through 127 characters.

---

statistics [name *service_name* **]**

name *service_name*: Displays MAG service statistics for an existing MAG service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view configuration information for MAG services on this system.

Example

The following command displays service statistics for the MAG service named *mag1*:

```
show mag-service name mag1
```

show map-service

Displays information configured for the Mobile Application Part (MAP) services, including MAP service features and operational configuration. Also includes some related configuration information for the HLR and EIR configuration parameters.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show map-service [all | name *srvc_name* **] [| { grep** *grep_options* **| more }]**

name *srvc_name*

Specifies an existing MAP service as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display all MAP service or the statistics for a particular MAP service.

Example

The following command displays configuration information for the MAP service named *map-svc-1*:

```
show map-service name map-srv-1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show map statistics

Displays Mobile Application Part (MAP) statistics.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show map statistics [name *srvc_name* **[| { grep** *grep_options* **| more }]**

name *srvc_name*

Specifies an existing MAP service as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display all MAP statistics or the statistics for a particular MAP service.

Example

The following command displays statistics for the MAP service named *map-svc-1*:

```
show map statistics name map-svc-1
```

The following command displays combined statistics for all MAP services in the current context:

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show maximum-temperatures

Shows the maximum temperature reached by each card since the last temperature timestamp reset.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show maximum-temperatures [verbose] [| { grep *grep_options* **| more }]**

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

verbose

Indicates that the output is to contain detailed information.

Usage

Verify the maximum temperature reached by components in the chassis since the indicated timestamp.

Important: This command is not supported on all platforms.

Example

```
show maximum-temperatures

show maximum-tempteratures verbose
```

show mbms bearer-service

Displays configuration information for bearer services configured for the multimedia broadcast multicast service (MBMS) running on this system.

Product

GGSN, SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show mbms bearer-service [all | apn *apn_name* **mcast-addr** *ip_address* **| service-type { broadcast | multicast } | full | instance** *instance_id* **| summary] + [| { grep** *grep_options* **| more }]**

all

Displays information on all bearer services configured on the system.

apn *apn_name* **mcast-addr** *ip_address*

Displays bearer service information of the MBMS for a specific Access Point Name (APN). *apn_name* is bound to a given BM-SC (Broadcast Multicast - Service Center) server address *ip_address*.
apn_name is the name of the APN expressed as an alphanumeric string of 1 through 62 characters that is case sensitive.
ip_address is the IP address of the BM-SC server in IPv4 dotted-decimal notation bound to the APN.

service-type { broadcast | multicast }

Displays information for a specific type of service for MBMS.
broadcast: Specifies the MBMS service type as broadcast only.
multicast: Specifies the MBMS service type as multicast only.

full

Displays full information for specific or all instances of bearer service in MBMS feature on system.

instance *instance_id*

Displays session information filtered for an instance of a bearer service running as an MBMS session and specified an integer from 1 through 64.

summary

Displays summary information for specific or all instances of a bearer service.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more** options, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to verify the configuration of one or all bearer services and active instances of bearer services under MBMS. It is also useful for monitoring or troubleshooting purposes.
If this command is executed from within the local context with the **all** keyword, information for all bearer service instances running under MBMS will be displayed.

Example

The following command displays configuration information for all bearer service instances running on system:

```
show mbms bearer-service full all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show mipfa

Displays information for specified Mobile IP Foreign Agent (MIP-FA) calls.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show mipfa { [[counters | full | summary] { all | callid *call_id* **| msid** *ms_id* **| peer-address [** *operator* **]** *peer_address* **| reverse-tunnel { on | off } | username** *user_name* **} | statistics [fa-service** *fa_name* **| peer-address [** *peer_address* **| greater-than** *peer_address* **| less-than** *peer_address* **| >** *peer_address* **| <** *peer_address* **] }] | peers fa-service** *service_name* **[current-sessions { { >** *sessions* **[<** *sessions* **] | { <** *sessions* **[>** *sessions* **] |** *sessions* **}] [peer-address** *address* **] } [| { grep** *grep_options* **| more }]**

---

counters | full | summary

counters: Displayed output includes the statistical counters.
full: Displays detailed information.
summary: Displays only summary information. this is the default setting.
These options are not available in conjunction with the **statistics** keyword.

---

all | callid call_id | msid *ms_id* **| peer-address** *peer_ip_address* **| reverse-tunnel { on | off } | username** *user_name*

all: Displays all available information.
callid *call_id*: Displays information only for calls with the call ID specified as a 4-byte hexadecimal number.
msid *ms_id*: Displays information for a mobile subscriber ID expressed as a string from 7 to 16 digits for an IMSI, MIN, or RMI and/or characters $ and * for wildcard filter.
show mipha msid *01234567$$*
Shows any subscriber with an MSID that matches the upper 8 digits of the supplied MSID, such as 01234567, and any two digits at the remaining two places.
peer-address *peer_ip_address*: Displays information for the MIP call for the peer IP address specified using IPv4 dotted-decimal notation.
reverse-tunnel { **on** | **off** }: Enables the display of reverse IP tunnel information.
username *user_name*: Displays MIP call user information for the username specified as an alphanumeric string of 1 through 127 characters that may include wildcard characters ($ and *).

---

statistics [fa-service *fa_name* **| peer-address [peer_address | greater-than** *peer_address* **| less-than** *peer_address* **| >** *peer_address* **| <** *peer_address* **]**

Displays information for the foreign agent service specified by name or peer IP address.
fa-service *fa_name* must be an alphanumeric string of 1 through 63 characters.
peer-address *peer_address* must be specified using IPv4 dotted-decimal notation.
greater-than *peer_address*: Specifies the range of IPv4 addresses greater than *peer_address.*
less-than *peer_address*: Specifies the range of IPv4 addresses less than *peer_address.*
> *peer_address*: Specifies the range of IPv4 addresses greater than *peer_address.*
< *peer_address*: Specifies the range of IPv4 addresses less than *peer_address.*

peer-address [*operator* **]** *peer_address*

In conjunction with the **mipfa [summary] peer-address** keyword, indicates a range of peers is to be displayed.
peer-address [*operator* **]** *peer_address* must be specified using IPv4 dotted-decimal notation.
operator implies how to logically specify a range of peer-address and it must be one of the following:

- **<**: IP address is less than the specified *peer_address*
- **>**: IP address is greater than the specified *peer_address*
- **greater-than**: IP address is greater than the specified *peer_address*
- **less-than**: IP address is less than the specified *peer_address*

peers fa-service *service_name* **[current-sessions { { > | greater-than }** *sessions* **[<** *sessions* **] | { < | less-than }** *sessions* **[>** *sessions* **] |** *sessions* **}] [peer-address** *address* **]**

Displays peer servers for the specified FA service.
fa-service *service_name*: Specifies the name of an existing FA service for which the associated peer servers are to be displayed as an alphanumeric string of 1 through 63 characters.
current-sessions: Displays only peer servers with current sessions meeting the following criteria:

- > | greater-than *sessions*: Displays only peer servers currently running sessions higher than the value entered in this parameter. *sessions* must be an integer from 1 to 3000000. **Note**: the keyword "**greater-than**" and the "**>**" symbol are interchangeable in this instance of the command.
- **<** *sessions*: Displays only peer servers that are currently running sessions l than the **greater-than** parameter but less than the value entered in this parameter. *sessions* must be an integer from 1 to 3000000.
- < | less-than *sessions*: Displays only peer servers currently running sessions lower than the value entered in this parameter. *sessions* must be an integer from 1 to 3000000. **Note**: the keyword "**less-than**" and the "**<**" symbol are interchangeable in this instance of the command.
- > *sessions*: Displays only peer servers that are currently running sessions lower than the **less-than** parameter but more than the value entered in this parameter. *sessions* must be an integer from 1 to 3000000.
- *sessions*: Displays only peer servers currently running sessions that are equal to the value entered in this parameter. *sessions* must be an integer from 1 to 3000000.

peer-address *address*: Displays only peer servers matching the IP address entered in this parameter. *address* must be specified using IPv4 dotted-decimal notation and can be followed by the netmask of the address.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View MIP foreign agent information to support troubleshooting subscriber issues by viewing call information and filtering on the subscriber information using various methods.

Example

The following displays the call information for all mobile IP FA calls and statistics for *fa1*, respectively:

show mipfa all

The following command displays the statistics for the foreign agent service *fa1*:

show mipfa statistics fa-service fa1

The following commands displays call information for user *user6@aaa* in full detail and in summary:

show mipfa full username user6@aaa

show mipfa summary username user1

The following displays MIP FA call information for calls from mobile subscriber *4412345678* and peer address *10.2.3.4*, respectively:

show mipfa msid 4412345678 *4412345678*

show mipfa peer-address 10.2.3.4

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show mipha

Displays information for specified Mobile IP Home Agent (MIP-HA) calls.

Product

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show mipha { [[counters | full | summary] { all | callid *call_id* **| imsi** *imsi_num* **| ip-address** *ip_addr* **| msid** *msid_num* **| peer-address [** *operator* **]** *peer_address* **| reverse-tunnel { on | off } | username** *user_name* **} | statistics [ha-service** *ha_name* **| peer-address** *peer_address* **] }] | peers ha-service** *service_name* **[current-sessions { { > | greater-than }** *sessions* **[<** *sessions* **] | { < | less-than }** *sessions* **[>** *sessions* **] |** *sessions* **}] [peer-address** *address* **] } [| { grep** *grep_options* **| more }]**

---

counters | full | summary

Default: concise output.
counters: Displayed output includes the statistical counters.
full: Displays detailed information.
summary: Displays only summary information.
These options are not available in conjunction with the **statistics** keyword.

---

msid *msid_num*

Displays information for the subscriber with the supplied MSID on HA.
msid *msid_num* specifies a mobile subscriber ID for which information is to be displayed. *ms_id* must be from 7 to 16 digits for an IMSI, MIN, or RMI and /or characters $ and * for wildcard filtering.
If **enforce imsi-min equivalence** is enabled on the chassis and MIN or IMSI numbers are supplied, this keyword/ filter will show subscribers with a corresponding MSID (MIN or IMSI) whose lower 10 digits matches the lower 10 digits of the supplied MSID.
show mipha msid *ABCD0123456789* or
show mipha msid *0123456789*
Shows any subscriber with a MSID that match the lower 10 digits of MSID supplied, such as 0123456789.
show mipha msid *01234567$$*
Shows any subscriber with a MSID that match the upper 8 digits of the supplied MSID, such as 01234567 and any two digits at the remaining two places.

---

all | callid *call_id* **| imsi** *imsi_num* **| ip-address** *ip_addr* **| msid** *msid_num* **| peer-address [** *operator* **]** *peer_address* **| reverse-tunnel { on | off } | username** *user_name*

all: Displays all available information.
callid *call_id*: Displays information only for calls with the call ID specified as a 4-byte hexadecimal number.
imsi *imsi_num*: Specifies an IMSI (international mobile subscriber ID) for which information is to be displayed. The IMSI is a 15-character field which identifies the subscriber's home country and carrier.
ip-address *ip_addr*: Displays statistics for a call with the IP address specified in IPv4 dotted-decimal notation.

msid *msid_num*: Specifies a mobile subscriber ID only for which information is to be displayed. *ms_id* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI.
peer-address *peer_address*: Displays statistical information for the peer IP address specified using IPv4 dotted-decimal notation.
reverse-tunnel { **on** | **off** }: Enables the display of reverse IP tunnel information.
username *user_name*: Displays user MIP call information for the username specified as an alphanumeric string of 1 through 127 characters including wildcard characters ($ and *).

---

peer-address [*operator* **]** *peer_address*

In conjunction with **mipha [summary] peer-address** keyword, indicates a range of peers is to be displayed.
peer_address must be specified using IPv4 dotted-decimal notation.
operator implies how to logically specify a range of peer-addresses and it must be one of the following:

- **<**: IP address is less than the specified *peer_address*
- **>**: IP address is greater than the specified *peer_address*
- **greater-than**: IP address is greater than the specified *peer_address*
- **less-than**: IP address is less than the specified *peer_address*

---

statistics [ha-service *ha_name* **| peer-address** *peer_address* **]**

Displays statistical information for the home agent service specified by its name (an alphanumeric string of 1 through 63 characters) or peer IP address (IPv4 notation).

---

peers ha-service *service_name* **[current-sessions { { > | greater-than }** *sessions* **[<** *sessions* **] | { < | less-than }** *sessions* **[>** *sessions* **] |** *sessions* **}] [peer-address** *address* **]**

Displays peer servers for the specified HA service.
ha-service *service_name*: Specifies the name of an existing HA service for which the associated peer servers are to be displayed as an alphanumeric string of 1 through 63 characters.
current-sessions: Displays only peer servers with current sessions meeting the following criteria:

- > | greater-than *sessions*: Displays only peer servers currently running sessions higher than the value entered in this parameter. *sessions* must be an integer from 1 to 3000000. **Note**: the keyword "**greater-than**" and the "**>**" symbol are interchangeable in this instance of the command.
- **<** *sessions*: Displays only peer servers that are currently running sessions higher than the **greater-than** parameter but less than the value entered in this parameter. *sessions* must be an integer from 1 to 3000000.
- < | less-than *sessions*: Displays only peer servers currently running sessions lower than the value entered in this parameter. *sessions* must be an integer from 1 to 3000000. **Note**: the keyword "**less-than**" and the "**<**" symbol are interchangeable in this instance of the command.
- > *sessions*: Displays only peer servers that are currently running sessions lower than the **less-than** permitter but more than the value entered in this parameter. *sessions* must be an integer from 1 to 3000000.
- *sessions*: Displays only peer servers currently running sessions that are equal to the value entered in this parameter. *sessions* must be an integer from 1 to 3000000.

peer-address *address*: Displays only peer servers matching the IP address entered in this parameter. *address* must be specified using IPv4 dotted-decimal notation and can be followed by the netmask of the address.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View MIP home agent information to support troubleshooting subscriber issues by viewing call information and filtering on the subscriber information using various methods.

Example

The following displays the call information for all mobile IP HA calls and statistics for *ha1*, respectively:

```
show mipha all

show mipha statistics ha-service ha1
```

The following commands displays call information for user *isp1user1* in full detail and in summary:

```
show mipha full username isp1user1

show mipha summary username user1
```

The following displays MIP-HA call information for calls from mobile subscribers with reverse tunneling *off* and peer address *10.2.3.4*, respectively:

```
show mipha reverse-tunnel off

show mipha peer-address 10.2.3.4
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show mipv6ha

Displays information for specified Mobile IPv6 Home Agent (MIPv6-HA) calls.

Product

PDSN, HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show mipv6ha [all | callid *callid* **| counters** *filter* **| full** *filter* **| ipv6-address** *ip_addr*| **statistics mipv6ha-service** *mipv6ha-service_name* **| summary** *filter* **| username** *user_name* **]**

---

all

Displays all information for MIPv6-HA calls.

---

callid *call_id*

Specifies the Call Identification number as an 8-digit hexadecimal number.

---

counters [all | callid | ipv6-address | username]

Displays the counters associated with the MIPv6-HA service. The following filters are available:

- **all**
- **callid:**
- **ipv6-address**
- **username**

---

full [all | callid | ipv6-address | username]

Displays all available information for the associated display or filter keyword.
The following filters are available:

- **all**
- **callid:**
- **ipv6-address**
- **username**

---

ipv6-address *ip_addr*

Displays information for subscribers connected via the packet control function for a specific or range of IPv6 addresses. The address must be specified using the IPv6 colon-separated notation.

- **<**: Filters output so that only information less than the specified IPv6 address value is displayed.
- **>**: Filters output so that only information greater than the specified IPv6 address value is displayed.
- **less-than**: Filters output so that only information less than the specified IPv6 address value is displayed.
- **greater-than**: Filters output so that only information greater than the specified IPv6 address value is displayed.

statistics [mipv6ha-service *mipv6ha-service_name* **]**

Displays all information collected for specific protocol since last the **restart** or **clear** command. This can be filtered according to a specified **mipv6ha-service**.

summary [all | callid | ipv6-address | username]

Displays summary information for defined sessions, based on defined parameters.
The following filters are available:

- **all**
- **callid:**
- **ipv6-address**
- **username**

username *user_name*

Displays session information for a specific username.

Usage

View MIPv6 home agent information to support troubleshooting subscriber issues by viewing call information and filtering on the subscriber information using various methods.

Example

The following displays the call information for all mobile IPv6 HA calls:

```
show mipv6ha all
```

The following command displays call information for user *mipv6hauser1* in full detail and in summary:

```
show mipv6ha full username mipv6hauser1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show mme-service

Displays configuration information for Mobility Management Entity (MME) services on this system.

Product

MME

Privilege

Inspector

Syntax

show mme-service { all | name *svc_name* **} [| { grep** *grep_options* **| more }]**

all

Displays configuration information for all MME services configured on this system.

name *service_name*

Displays configuration information for an existing MME service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to view configuration information for MME services on this system.

Example

The following command displays service statistics for the MME service named *mme1*:

```
show mme-service name mme1
```

Important: Output descriptions for these commands are available in the *Statistics and Counters Reference*.

show mme-service db record

Displays the Mobile Management Entity (MME) database records for MME sessions grouped in session instances on this system and filtered with IMSI or GUTI as criteria.

Product

MME

Privilege

Inspector

Syntax

show mme-service db record { all | call-id *call_id* **| guti plmn** *plmn_id* **group-id** *mme_grp_id* **code** *mme_code* **m-tmsi** *mtmsi_value*| **imsi** *imsi_identifier*

all

Displays all database records of a session instance used for MME service.

call-id *call_id*

Displays database records filtered by the call ID specified as an 8-digit hexadecimal number

guti plmn *plmn_id* **group-id** *mme_grp_id* **code** *mme_code* **m-tmsi** *mtmsi_value*

Displays database records filtered by the Globally Unique Temporary Identifier (GUTI). The GUTI is constructed from the GUMMEI and the M-TMSI.
The GUMMEI is constructed from the public land mobile network (PLMN) ID [MMC and MNC] and the MME Group ID (MMEGI). Within the MME, the mobile is identified by the M-TMSI.
A GUTI has: 1) a unique identity for the MME which allocated the GUTI; and 2) the unique identity of the UE within the MME that allocated the GUTI.
The MME Identifier (MMEI) is constructed from an MME Group ID (MMEGI) and an MME Code (MMEC).

imsi *imsi_identifier*

Displays database records filtered by International Mobile Subscriber Identity (IMSI).
imsi_identifier is a 15-character IMSI field which identifies the subscriber's home country and carrier. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘). For example; ‘$’.

Usage

Use this command to view database records for all or a particular instance of session manager for MME services on this system with IMSI or GUTI as a filter criteria.

Example

The following command displays the summary database records of a session instance for a subscriber having IMSI as *123455432112345* in the MME service:

```
show mme-service db record imsi 123455432112345
```

Important: Output descriptions for these commands are available in the *Statistics and Counters Reference*.

show mme-service db statistics

This command displays the Mobile Management Entity (MME) database statistics for all or specific MME sessions on this system.

Product

MME

Privilege

Inspector

Syntax

show mme-service db statistics [instance *smgr_instance* **]**

instance *smgr_instance*

Displays MME database statistics for a specific instance of a session manager running the MME service. *smgr_instance* is an instance ID specified as an integer from 0 through 4294967295. If an instance is not specified, summary statistics are displayed.

Usage

Use this command to view database statistics for all or a particular instance of session manager for MME services on this system.

Example

The following command displays summary database statistics for the MME service running on a system:

```
show mme-service db statistics
```

Important: Output descriptions for these commands are available in the *Statistics and Counters Reference*.

show mme-service enodeb-association

Displays configuration information for an eNodeB association within an MME service.

Product

MME

Privilege

Inspector

Syntax

show mme-service enodeb-association [summary | full] [all | | ipsec | mme-service-name *mme_svc_name* **| peer-address** *peer_ip_address* **| peer-id** *peer_identifier* **] [| { grep** *grep_options* **| more }]**

---

summary

Displays summarized output for this command.

---

full

Displays detailed output for this command.

---

all

Displays information of all eNodeBs associated with MME services on this system.

---

ipsec

Displays information of all IPSec enabled eNodeBs associated with MME services on this system.

---

mme-service-name *mme_svc_name*

Displays summarized or detailed configuration information for eNodeBs associated with an existing MME service specified as an alphanumeric string of 1 through 63 characters.

---

peer-address *peer_ip_address*

Displays summarized or detailed configuration information of eNodeBs associated with an existing MME peer IP address configured with an MME service and expressed in IPv4 dotted-decimal or IPv6 colon-separated notation.

---

peer-id *peer_identifier*

Displays summarized or detailed configuration information for eNodeBs associated with a an existing MME peer ID configured with an MME service and specified as an integer from 1 through 4294967295.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to view configuration information of eNodeBs associated with an MME service on this system.

Example

The following command displays detailed service statistics for associated eNodeBs within the MME service named *mme1*:

```
show mme-service enodeb-association full mme-service-name mme1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show mme-service session

Displays session information for Mobile Management Entity (MME) service(s) running on a peer or local system.

Product

MME

Privilege

Inspector

Syntax

show mme-service session [summary | full | counters] [all | callid *call_identifier* **| imei** *imei_id* **| imsi** *imsi_id* **| ipsec | mme-service** *service_name* **| msisdn** *number* **| pdn-address** *pdn_ip_address* **| s1-peer** *s1_peer_ip_address* **| s11-peer** *s11_peer_ip_address* **| vlr-name** *vlr_name* **| ue-ecm-state { connected | idle }] [| { grep** *grep_options* **| more }]**

summary

Displays summarized output for this command.

full

Displays detailed output for this command.

counters

Displays all counters for related events and messages for an MME session running on a system.

all

Displays information for all MME sessions running on this system.

callid *call_identifier*

Displays summarized or detailed configuration information for an MME session filtered by a call identifier within an MME service configured on this system.
call_identifier must be an existing call identity in 8-digit hexadecimal format running in an MME service on this system.

imei *imei_id*

Displays summarized or detailed configuration information about MME sessions running and filtered by an International Mobile Equipment Identification (IMEI) number within an MME service configured on this system.
imei_id must be an existing IMEI in an existing MME service on the system. *imei_id* must contain an 8-digit TAC (Type Allocation Code) and a 6-digit SNR (Serial Number).

imsi *imsi_id*

Displays summarized or detailed configuration information about MME sessions running and filtered by an International Mobile Subscriber Identity (IMSI) number within an MME service configured on the system.
imsi_id must be an existing IMSI in an existing MME service on the system. *imsi_id* is a 15-character IMSI field which identifies the subscriber's home country and carrier.

Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘). For example; ‘$’.

ipsec

Displays information for all IPSec enabled sessions using MME services on the system.

mme-service *service_name*

Displays summarized or detailed configuration information about MME sessions running and filtered by an MME service name configured on the system.
service_name must be a configured MME service on the system, expressed as an alphanumeric string of 1 through 63 characters.

msisdn *number*

Displays summarized or detailed configuration information about MME sessions running and filtered by a Mobile Station International ISDN Number.
number must be a combination of the CC (Country Code) and National (significant) mobile number, not exceeding 15 digits.

pdn-address *pdn_ip_address*

Displays summarized or detailed configuration information about MME sessions running and filtered by the IP address of a connected PDN(s) within an MME service configured on this system.
pdn_ip_address must be a configured IP address of a PDN expressed in IPv4 dotted-decimal or IPv6 colon-separated notation within an existing MME service on the system.

s1-peer *s1_peer_ip_address*

Displays summarized or detailed configuration information of MME sessions running and filtered by the IP address of a peer connected through an S1 interface within an MME service configured on this system.
s1_peer_ip_address must be a configured IP address of a peer on S1 interface expressed in IPv4 dotted-decimal or IPv6 colon-separated notation within an existing MME service on this system.

s11-peer *s11_peer_ip_address*

Displays summarized or detailed configuration information of MME sessions running and filtered by IP address of a peer connected through S11 interface with an MME service configured on this system.
s11_peer_ip_address must be a configured IP address of a peer on S11 interface expressed in IPv4 dotted-decimal or IPv6 colon-separated notation within an existing MME service on this system.

vlr-name *vlr_name*

Displays summarized or detailed configuration information of MME sessions running and filtered by Visitor Location Register (VLR) name.
vlr_name must be an alphanumeric string of 1 through 63 characters.

ue-ecm-state { connected | idle }

Displays summarized or detailed configuration information about MME sessions running and filtered by the UE’s EPS Connected Management (ECM) state.
connected: Specifies that summarized or detailed configuration information about MME sessions is to be displayed based on the UE ECM state of “connected”.

idle: Specifies that summarized or detailed configuration information about MME sessions is to be displayed based on the UE ECM state of "idle".

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to view information for MME sessions within MME services on this system.

Example

The following command displays detailed session statistics for an MME service running on this system:

```
show mme-service session full
```

Important: Output descriptions for these commands are available in the *Statistics and Counters Reference*.

The following command displays detailed session counters for an MME service running on this system:

```
show mme-service session counters
```

show mme-service statistics

This command displays the service statistics of an MME service specified by various criteria.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

show mme-service statistics [sctp [mme-service *mme_svc_name* **] | s1ap [mme-service** *mme_svc_name* **| peer-id** *peer_identifier* **] | [emm-only | esm-only] [mme-service** *mme_svc_name* **| peer-id** *peer_identifier*] **| handover] [verbose] [| { grep** *grep_options* **| more }]**

emm-only

Filters the output of EPS mobility management (EMM) related statistics by an MME service name or peer MME identifier.

esm-only

Filters the output of EMM related statistics by MME service name or peer MME identifier.

s1ap

Filters the output of S1-AP statistics by MME service name of peer MME identifier.

sctp

Filters the output of SCTP statistics by MME service name of peer MME identifier.

mme-service *mme_svc_name*

Filters the output of all MME service statistics (such as EMM, ESM, SCTP, S1-AP, and SCTP) by MME service name.

peer-id *peer_identifier*

Filters the output of all MME service statistics (such as EMM, ESM, SCTP, S1-AP, and SCTP) by MME peer identifier.

handover

Filters the output of all handover statistics (such as Intra-MME, EUTRAN<->EUTRAN via S10, EUTRAN<->UTRAN via GnGp, EUTRAN<->GERAN via GnGp, and EUTRAN<->UTRAN via S3) by an MME service.

verbose

Displays comprehensive information for a specific argument or set of arguments.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

This command is used to display the statistical information of an MME service based on various filter criteria as a local MME service or a peer MME related to EMM, ESM, SCTP, S1-AP, and SCTP.

Example

The following command displays the service session statistics of all MME service on a system related to all; such as EMM, ESM, SCTP, S1-AP, and SCTP:

```
show mme-service statistics
```

Important: Output descriptions for these commands are available in the *Statistics and Counters Reference*.

The following command displays the service session statistics of all MME services on a system related to S1-AP:

```
show mme-service statistics s1ap
```

The following command displays the service session statistics of all MME services on a system related to EMM only:

```
show mme-service statistics emm-only
```

show mpls ldp

Displays the Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) information.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
show mpls ldp { bindings { ldp-id IPv4_add | local [ ldp-id | local | prefix | remote ] |
prefix IPv4_addr | remote } | discovery | neighbor { detail | ldp-id } }
```

bindings

Displays the MPLS LDP label bindings.

ldp-id

Displays label values for a specific peer LDP ID.

local

Displays locally assigned label values.

prefix

Displays label values for a specific prefix.

remote

Displays remotely assigned label values.

discovery

Displays the MPLS LDP discovery information.

neighbor

Displays the MPLS LDP peer information.

detail

Displays the MPLS LDP peer information in details. The displayed information includes, Local LDP ID, Peer LDP ID, Transport address, State (for example, Established), Role (for example, Active), Uptime, Keepalive negotiated hold time, Proposed Local/Peer, Remaining Keepalive hold time, and Address advertised.

Usage

This command displays statistical information for an MPLS Label Distribution Protocol configuration. The information includes Prefix, LDP ID, Label, Nexthop, and Egress_if_index for all MPLS LDP Bindings configurations.

Example

The following command displays information about MPLS LDP protocol related configurations:

```
show mpls ldp discovery neighbor ldp-id 10.2.3.4 detail bindings ldp-id
31.32.33.34 prefix 192.168.102.232 local remote
```

The following command displays the MPLS LDP discovery information, including, LDP Peer IDs, Hold time (in seconds), Proposed Local/Peer, and Remaining (time in seconds):

```
show mpls ldp discovery
```

The following command displays the remotely assigned label values in the MPLS LDP binding configuration:

```
show mpls ldp bindings remote
```

Important: Output descriptions for these commands are available in the *Statistics and Counters Reference*.

show mseg-config

Displays Mobile Services Edge Gateway (MSEG) configuration information.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show mseg-config all [| { grep *grep_options* **| more }]**

all

Displays all available MSEG configuration information.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to view MSEG configuration information.

show mseg-service

Displays Mobile Services Edge Gateway (MSEG) service configuration information.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show mseg-service { all | name *mseg_service_name* **} [| { grep** *grep_options* **| more }]**

all

Displays configuration information for all MSEG services.

name *mseg_service_name*

Displays configuration information for the specified MSEG service.
mseg_service_name must be the name of a configured MSEG service, expressed as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to view MSEG service configuration information.

Example

The following command displays configuration information for the MSEG service named *standard*:

```
show mseg-service name standard
```

show multicast-sessions

Displays information for multicast sessions defined by the specified keywords.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show multicast-sessions [*command_keyword* **] [** *filter_keywords* **] [| { grep** *grep_options* **| more }**

command_keyword

The following keywords are base commands that each have a distinct display output. Only one keyword can entered on the command line.

debug-info { callid *id* **| flowid** *id* **}**

Displays internal call troubleshooting information for multicast sessions defined by the specified keywords.
callid *id:* Displays subscriber information for the call specified as an 8-digit hexadecimal number.
flowid *id:* Displays information for a specific BCMCS flow, defined by The flow ID as a hexadecimal number.

full

Displays all available multicast session information. The following filter keywords are valid for this command: active, all, callid, card-num, dormant, flowid, flowid-type, mcast-address, pcf, pdsn-service, grep, more

summary

Only displays a summary of multicast session information. The following commands are valid for this command: active, all, callid, card-num, dormant, flowid, flowid-type, mcast-address, pcf, pdsn-service, grep, more

filter_keywords

The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all Command Keywords. Multiple Filter Keywords can be entered on a command line. When multiple Filter Keywords are specified, the output conforms to all of the Filter Keywords specifications.

active

Only displays information for multicast sessions that are currently active.

all

If no keywords are specified before **all**, information for all multicast sessions is displayed. If keywords are specified before **all**, all information is displayed with no further options being allowed.

callid *id*

Displays multicast session information for the call specified by *id*. The call must be specified as an 8-digit hexadecimal number.

card-num *card_num*

The slot number of the processing card by which the subscriber session is processed. *card_num* is a slot number from 1 through 7 or 10 through 16.

dormant

Shows information for subscriber sessions that are dormant (not transmitting or receiving data).

flowid *id*

Displays information for a specific BCMCS flow, defined by *id*. The flow ID must be a hexadecimal number.

flowid-type [flow | program]

Displays information for multicast sessions according to the type of flow.
flow: Shows all multicast sessions for the flow ID type "flow".
program: Shows all multicast sessions for the flow ID type "program".

mcast-address *ipv4_address*

Show multicast sessions for a specific multicast address. Must be followed by the IP address of an interface, using IPv4 dotted-decimal notation.

pcf *ipv4_address*

Displays information for multicast sessions connected via the packet control function, defined by *ipv4_address*. The address must be specified using IPv4 dotted-decimal notation.

pdsn-service *svc_name*

Displays information for multicast session connected to the packet data service *svc_name*.The packet data service must have been previously configured and expressed as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
Please refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

Usage

Use this command to view information about multicast sessions.
The output of this command may be considered for part of a periodic system auditing program by verifying active and dormant sessions.

Example

The following command displays the all broadcast-multicast sessions active in a context/system:

```
show multicast-sessions all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show network-requested-pdp-context

Displays information for the specified network-requested packet data protocol (PDP) context.

Product

GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show network-requested-pdp-context imsi *imsi_value*

imsi *imsi_value*

Specifies that information will be displayed for a particular International Mobile Subscriber Identity (IMSI). *imsi_value* is an integer from 1 to 15 digits.

Usage

USe this command to display information pertaining to network-requested PDP contexts.

Example

The following command displays network-requested PDP context information for a subscriber with an IMSI of *123456789*:

```
show network-requested-pdp-context imsi 123456789
```

show network-service-entity

Displays information regarding the network service entities (NSEs) in the network.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show network-service-entity { consolidated-status | fr-config [ peer-nsei nsei] | ip-
config [ nsvl { all | instance value } ] }
```

consolidated-status

Displays Network Service Virtual Connection (NSVC) status information for all network service entities in the network. This keyword is particularly useful for troubleshooting.

fr-config [peer-nsei *nsei*]

Displays network service configurations for NSEs using Frame Relay configurations.
peer-nsei *nsei* limits the display to a specific peer NSE identified as an integer from 0 through 65535.

ip-config [nsvl { all | instance *value* }

Displays network service configurations for NSEs using IP configurations.
Including the **nsvl** keyword limits the display to all or a single (instance 0 to 3) of a network service virtual link.

Usage

Use this command to display NSE information pertaining to the NSVCs of the NSEs in the networks or NSEs configured for Frame Relay or IP.

Example

The following command displays the status of all the NSVCs for all the NSEs in the network.

```
show network-service-entity consolidated-status
```

show npu error-counters

Displays packet error counters.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show npu error-counters [| { grep *grep_options* **| more }]**

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View network timing protocol information to troubleshooting system clock issues by displaying the associations and status of the local NTP client.

Example

The following displays the NPU information.

show npu error-countersshow npu error-counters |grep *qwe*

show npu utilization

Displays NPU information utilization.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show npu utilization table [| { grep *grep_options* **| more }]**

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View network timing protocol information to troubleshooting system clock issues by displaying the associations and status of the local NTP client.

Example

The following displays the NPU information.

show npu utilization table

show npu utilization table | grep *qwe*

show ntp

Displays the network timing protocol (NTP) associations and status.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ntp { associations | status } [address *ip_address* **] [| { grep** *grep_options* **| more }]**

associations

Displays the current NTP server associations and related statistics.

status

Displays the client permeates configured and the synchronization status.

address *ip_address*

Specifies the IP address of an NTP server/client in the current context in IPv4 dotted-decimal notation.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View network timing protocol information to troubleshooting system clock issues by displaying the associations and status of the local NTP client.

Example

The following displays the NTP associations and status, respectively.

```
show ntp associationsshow ntp status
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show nw-reachability server

Displays the configuration of network reachability servers for the current context.

Product

HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show nw-reachability server { all | name server_name }
```

all

Displays configuration information for all network reachability servers in the current context.

name *server_name*

Displays configuration information for an existing network reachability server specified as an alphanumeric string of 1 through 15 characters.

Usage

Use this command to display configuration information on network reachability servers configured in the current context.

Example

The following command displays information on all network reachability servers in the current context:

```
show nw-reachability server all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show operator-policy

Displays the information configured for an operator policy.

Product

MME, S-GW, SGSN

Privilege

Inspector

Syntax

show operator-policy { all | full { all | name *op_policy_name* **} | name** *op_policy_name* **} [| { grep** *grep_options* **| more }]**

---

all

Displays a list of all operator policies configured on the system.

---

full { all | name *op_policy_name* **}**

full:Displays a full set of available information for the specified operator policy (policies).
all: Displays a full set of available information for all operator policies configured on the system.
name *op_policy_name*: Displays a full set of available information for an existing operator policy specified as an alphanumeric string of 1 through 64 characters.

---

name *op_policy_name*

Displays a full set of available information for an existing operator policy specified as an alphanumeric string of 1 through 64 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to display information for operator policies configured on the system. Operator policies are configured through the Global Configuration Mode and in the Operator Policy Configuration Mode. For more information regarding operator policy commands, refer to the *Operator Policy Configuration Mode Commands* chapter.

Example

The following command displays all available information for an operator policy named *policy-5*:

```
show operator-policy full name policy-5
```

show orbem

Displays information and statistics for the Object Request Broker Element Manager (ORBEM) interface in the current context.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show orbem { client { id *client_name* **| table } | event-notif-service filters | session { id** *session_name* **| table } | status } [| { grep** *grep_options* **| more }]**

---

client { id *client_name* **| table }**

Indicates the Common Object Request Broker Architecture (CORBA) client information is to be displayed. The keyword **table** is used to output to the display information on all configured clients. The keyword **id** is used to specify a specific client for which information is to be displayed specified as *client_name*.
client_name must refer to an existing client which is found using the **table** keyword option.

---

event-notif-service filters

Displays information pertaining to filters configured for the ORB Notification Service.

---

session { id *session_name* **| table }**

Indicates session information is to be displayed. The keyword **table** is used to output to the display information on all configured clients. The keyword **id** is used to specify a specific session for which information is to be displayed specified as *session_name*.
session_name must refer to an existing session which is found using the **table** keyword option.

---

status

Indicates that the ORBEM server status information is to be displayed.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Display current sessions when ORBEM system response may appear sluggish. This command is also useful in periodic verification of the server status.

Example

The following commands will display the information for all clients.

```
show orbem client table
```

The following commands display the information for the *clientName* and *sessionID*, respectively:

show orbem client id *clientName*

show orbem session id *sessionId*

The following command displays the ORBEM server status:

show orbem status

The following command displays the information for all sessions:

show orbem session table

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show patch-progress

Displays the status of the on-going software patch installation.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show patch-progress
```

Usage

Use this command to show the status of an on-going software patch installation.

Important: Software Patch Upgrades are not supported in this release.

show pcc-af service

Displays the statistical and configuration information of configured Policy and Charging Control- Application Function (PCC-AF) services configured in a context.

Product

IPCF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show pcc-af service [statistics] { all | name *pcc_af_svc_name* **| summary } [| { grep** *grep_options* **| more }]**

all

all: displays information for all configured PCC-AF services.

name *pcc_af_svc_name*

Displays information only for an existing PCC-AF service specified as an alphanumeric string of 1 through 79 characters

statistics

Displays the statistical information for a specific service or all PCC-AF services configured in a context.

summary

Displays the summarized output of this command.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to display the statistical and configuration information of configured PCC-AF services configured in a context.
Display can further be filtered for specific PCC-AF service name or summarized output of the command.

Example

The following command displays the information for the PCC-AF service named *pccApp1* in summarized output:

```
show pcc-af service name pccApp1 summary
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show pcc-af session

Displays the active/dormant session information about Policy and Charging Control- Application Function (PCC-AF) service instances configured and running on this system based on different filter criteria.

Product

IPCF

Privilege

Inspector

Syntax

show pcc-af sessions [full | summary] [all] [apn | call-id *call_id* **| ip-address** *pcc_af_ip_address* **| service** *pcc_af_svc_name* **| sipuri** *sip_uri* **]] [| { grep** *grep_options* **| more }]**

full

Displays the full information of specific registered IP Connectivity Access Network (IP-CAN) session(s) on a PCC-AF service instance running on system. Display can be filtered based on given filtering criteria.

summary

Displays summarized information for specific registered IP-CAN session(s) on a PCC-AF service instance running on system. Display can be filtered based on given filtering criteria.

all

Displays summarized or full information for all registered IP-CAN session(s) on a PCC-AF service instance running on system. Display can be filtered based on given filtering criteria.

apn *apn_name*

Displays information for PCC-AF service sessions connected via an existing APN at the Policy and Charging Enforcement Function (PCEF).

ip-address *pcc_af_ip_address*

Filters the display of full or summarized session statistics for IP-CAN session(s) based on the IP address of a registered PCC-AF server on a PCC-AF service instance.
pcc_af_ip_address is an IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated notation.

call-id *call_id*

Filters the display of full or summarized session statistics for IP-CAN session(s) based on the registered call ID on a PCC-AF service instance for the IP-CAN session subscriber in 8-digit hexadecimal format.

pcc-af-service *pcc_af_svc_name*

Filters the display of session statistics for a registered IP-CAN session(s) based on an existing PCC-AF service name specified as an alphanumeric string of 1 through 63 characters.

sipuri *sip_uri*

Displays summarized or full information for IP-CAN session(s) based on the SIP-URI on a PCC-AF service instance.
sip_uri is the Session Initiation Protocol (SIP) addressing schema to call another person. It resembles an e-mail address and is written in the SIP URI format as *sip:x@y:Port* format, where *x*=Username and *y*=host (domain or IP)

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to view the session statistics of all or specific registered IP-CAN session(s) or in selected part of user session for PCC-AF services configured and running on this system.

Example

The following command displays the summarized session statistics for all registered IP-CAN sessions on the PCC-AF service named *pccAF1*:

```
show pcc-af sessions summary all service pccAF1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show pcc-policy service

Displays the statistical and configuration information of configured PCC-Policy services configured in a context.

Product

IPCF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show pcc-policy service [statistics] { all | name *pcc_plcy_svc_name* **| summary } [| { grep** *grep_options* **| more }]**

---

all

all: displays information for all configured PCC-Policy services.

---

name *pcc_plcy_svc_name*

Displays information for an existing PCC-Policy service specified as an alphanumeric string of 1 through 79 characters.

---

statistics

Displays statistical information for a specific or all PCC-Policy services configured in a context.

---

summary

Displays summarized output for this command.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to display the statistical and configuration information of configured PCC-Policy services configured in a context.
Display can further be filtered for specific PCC-Policy service name or summarized output of the command.

Example

The following command displays the information for the PCC-Policy service named *pcc_policy1* in summarized output:

```
show pcc-policy service name pcc_policy1 summary
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show pcc-policy session

Displays active/dormant session information about PCC-Policy service instances configured and running on this system based on different filter criteria.

Product

IPCF

Privilege

Inspector

Syntax

show pcc-policy sessions [full | summary] [all] [apn | call-id *call_id* **| imsi** *imsi_id* **| ip-address** *pcc_pcef_ip_address* **| service** *pcc_plcy_svc_name* **]] [| { grep** *grep_options* **| more }]**

full

Displays full information for a specific registered IP Connectivity Access Network (IP-CAN) session(s) on a PCC-Policy service instance running on system. Display can be filtered based on given filtering criteria.

summary

Displays summarized information for a specific registered IP-CAN session(s) on a PCC-Policy service instance running on system. Display can be filtered based on given filtering criteria.

all

Displays summarized or full information for all registered IP-CAN session(s) on a PCC-Policy service instance running on system. Display can be filtered based on given filtering criteria.

apn *apn_name*

Displays information for PCC-Policy service sessions connected via an existing APN on the PCEF.

imsi *imsi_id*

Displays summarized or full information for IP-CAN session(s) based on the International Mobile Subscriber Identity (IMSI) of a subscriber in a PCC-Policy service instance.
imsi_id is the IMSI and must be a 15-character field which identifies the subscriber's home country and carrier.

ip-address *pcc_pcef_ip_address*

Filters the display of full or summarized session statistics for IP-CAN session(s) based on the IP address of the registered PCEF node specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

call-id *call_id*

Filters the display of full or summarized session statistics display for an IP-CAN session(s) based on the registered call ID in a PCC-Policy service instance.
call_id must be an existing call identifier in the IP-CAN session subscriber expressed in 8-digit hexadecimal format.

pcc-policy-service *pcc_plcy_svc_name*

Filters the display of session statistics for registered IP-CAN session(s) based on an existing PCC-Policy service name specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to view the session statistics for all or a specific registered IP-CAN session(s) for PCC-Policy services configured and running on this system.

Example

The following command displays summarized session statistics for all registered IP-CAN sessions on the PCC-Policy service named *pccPolicy1*:

```
show pcc-policy sessions summary all service pccPolicy1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show pcc-service

Displays the configuration information for Policy and Charging Control (PCC) services configured in a context.

Product

IPCF

Privilege

Security Administrator Operator, Inspector

Syntax

show pcc-service { summary | all | service-name *pcc_svc_name* **} [| { grep** *grep_options* **| more }]**

all

all: displays information for all configured PCC services.

service-name *pcc_svc_name*

Displays information for an existing PCC service specified as an alphanumeric string of 1 through 79 characters.

summary

Displays the summarized output of this command.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to display statistical and configuration information for configured PCC services in a context.
Display can further be filtered for a specific PCC- service name.

Example

The following command displays the information for the PCC service named *pcc_svc1*:

```
show pcc-service service-name pcc_svc1 summary
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show pcc-service session

Displays active/dormant session information about Policy and Charging Control (PCC) service instances configured and running on this system based on different filter criteria.

Product

IPCF

Privilege

Inspector

Syntax

show pcc-service sessions [full | summary] [all] [call-id *call_id* **| instance** *instance_id* **| service-name** *pcc_svc_name* **]] [| { grep** *grep_options* **| more }]**

full

Displays full information for a specific registered IP Connectivity Access Network (IP-CAN) session(s) in a PCC service instance running on system. Display can be filtered based on given filtering criteria.

summary

Displays summarized information for a specific registered IP-CAN session(s) in a PCC service instance running on system. Display can be filtered based on given filtering criteria.

all

Displays summarized or full information for all registered IP-CAN sessions on a PCC service instance running on system. Display can be filtered based on given filtering criteria.

instance *instance_id*

Displays summarized or full information for an IP-CAN session(s) based on the PCC service instance identifier on an IPCF/PCRF node specified as an integer from 1 through 512.

service-name *pcc_svc_name*

Filters the display of session statistics display of registered IP-CAN session(s) based on an existing PCC service name specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to view session statistics for all or a specific registered IP-CAN session(s) in PCC services configured and running on this system.

Example

The following command displays summarized session statistics for all registered IP-CAN sessions in the PCC service named *pccsvc1*:

```
show pcc-service sessions summary service-name pccsvc1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show pcc-service statistics

Displays the statistical information for Policy and Charging Control (PCC) services configured in a context.

Product

IPCF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show pcc-service statistics { all | service-name *pcc_svc_name* **[profile-name** *pcc_profile_name* **] } [| { grep** *grep_options* **| more }]**

all

Displays statistical information for all configured PCC services on a system.

service-name *pcc_svc_name*

Displays information for an existing PCC service specified as an alphanumeric string of 1 to 79 characters. It can be further filtered by the PCC profile name used in an IP-CAN session.

profile-name *pcc_profile_name*

Displays information for an existing PCC profile in an IP-CAN session.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to display the statistical information for PCC services configured in a context.
Display can further be filtered for a specific Profile name used in a session.

Example

The following command displays the information for the PCC service named *pcc_svc1* using PCC profile named *pcc_profile_default*:

```
show pcc-service statistics service-name pcc_svc1 profile-name
pcc_profile_default
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show pcc-sp-endpoint

Displays statistical and configuration information for a configured PCC Sp-Endpoint instance in a context.

Product

IPCF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show pcc-sp-endpoint [statistics] [all | name *sp_endpt_name* **] [| { grep** *grep_options* **| more }]**

all

Displays statistical information for all configured PCC Sp-Endpoint instances on a system.

name *sp_endpt_name*

Displays information for an existing PCC Sp-Endpoint instance specified as an alphanumeric string of 1 through 79 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to display statistical information for a configured PCC Sp-Endpoint instance in a context. Display can further be filtered for a specific PCC Sp-Endpoint instance used in a session.

Example

The following command displays statistical information for the PCC Sp-Endpoint instance named *Sp_Intf1*:

```
show pcc-sp-endpoint statistics name Sp_Intf1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show pcc-sp-endpoint connection

Displays statistical and configuration information for an Sp interface connection in a PCC Sp-Endpoint instance.

Product

IPCF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show pcc-sp-endpoint connection [ all | name sp_endpt_name [ peer sp_peer_name ] ] [ | { grep grep_options | more } ]
```

all

Displays statistical information for all configured PCC Sp-Endpoint instances on a system.

name *sp_endpt_name*

Displays information for an existing PCC Sp-Endpoint instance specified as an alphanumeric string of 1 through 79 characters. It can further be filtered with an Sp Endpoint peer (SSC/SPR) name used for the IP Connectivity Access Network (IP-CAN) session.

peer *ssc_name*

Displays information only for the PCC Sp-Endpoint instance within an existing Subscriber Service Controller/Subscriber Profile Repository (SSC/SPR) as a peer for an IP-CAN session.
ssc_name is the name of the SSC/SPR node used by the Sp Endpoint interface.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to display statistical information for Sp interface connections in PCC Sp-Endpoint instances.
Display can further be filtered for a specific peer name (SSC/SPR).

Example

The following command displays the Sp interface connection related statistical information for the PCC Sp-Endpoint instance named *Sp_Intf1* using peer name *SSC1*:

```
show pcc-endpoint connection name Sp_Intf1 peer SSC1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show pdg-service

Displays configuration information about Packet Data Interworking Function (PDIF) services configured on the system.

Product

PDG/TTG

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show pdg-service { all | name *service_name* **}**

all

Displays information for all configured Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) services.

name *service_name*

Displays information only for an existing PDG service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to display information for PDG services.

Example

The following command displays available information for all active PDG services:

```
show pdg-service all
```

show pdg-service statistics

Displays statistics for the Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) since the last **restart** or **clear** command. The output includes the number of each type of Extensible Authentication Protocol (EAP) messages.

Product

PDG/TTG

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show pdg-service statistics [name *service_name* **| peer-address** *ipv4_address* **]**

name *service_name*

Displays statistics for an existing PDG service specified an alphanumeric string of 1 through 63 characters.

peer-address *ipv4_address*

Displays statistics for a specific subscriber with the WLAN IP address specified in IPv4 dotted-decimal notation.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to display PDG service statistics.

Example

The following command displays statistics for all active PDG services:

```
show pdg-service statistics
```

show pdif-service

Displays configuration information about Packet Data Interworking Function (PDIF) services configured on the system.

Product

PDIF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show pdif service { all [counters] | name *name* **[counters] | statistics [name** *name* **| peer-address** *address* **] } [| { grep** *grep_options* **| more }]**

all [counters]

Displays configuration information and statistical counters for all PDIF services in the system.

name *name* **[counters]**

Displays configuration information and statistical counters for an existing PDIF service specified as an alphanumeric string of 1 through 63 characters.

statistics [name *name* **| peer-address** *address* **]**

name *name*: Displays service statistics for a an existing PDIF service specified as an alphanumeric string of 1 through 63 characters.
peer-address *address*: Displays service statistics for a peer server IP address specified in IPv4 dotted-decimal notation.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to display configuration information and statistics about PDIF services on the system.

Example

The following example displays configuration information about a PDIF service named *pdif23*:

```
show pdif service name pdif23
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show pdsn-service

Displays information for configured packet data services in the current context.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show pdsn-service { all | name pdsn_name } [ pcf-status [ address ip_address | filter [
all | icmp-monitored | no-calls | summary | up ] ] ] [ | { grep grep_options | more } ]
```

all | name *pdsn_name*

all: Displays information for all configured packet data services.
name *pdsn_name*: Displays information only for an existing PDSN service specified as an alphanumeric string of 1 through 79 characters.

pcf-status [address *ip_address* **| filter [all | icmp-monitored | no-calls | summary | up]]**

pcf-status: Displays summary information for all Packet Control Functions (PCFs).
address *ip_address:* Only lists information for the PCF with the IP address specified in IPv4 dotted-decimal notation.
filter: Filters the output so only the specified information is displayed. If a filter is specified with no keywords, summary information for all PCFs is displayed.

- **all**: Displays information for all the PCFs
- **icmp-monitored**: Displays information only for PCFs which are ICMP monitored
- **no-calls**: Displays information only for PCFs which have no active sessions
- **summary**: Displays only a summary of the status of the PCFs
- **up**: Displays information only for PCFs which are alive

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Show the PDSN service information for standard system monitoring or troubleshooting.

Example

The following will display the information for all configured services and *sampleService*, respectively:

```
show pdsn-service all

show pdsn-service name sampleService
```

show pgw-service

Displays configuration information for PDN Gateway (P-GW) services on this system.

Product

P-GW

Privilege

Inspector

Syntax

```
show pgw-service { all | name service_name | statistics { all | name service_name } [
verbose ] } [ | { grep grep_options | more } ]
```

all

Displays configuration information for all P-GW services configured on this system.

name *service_name*

Displays configuration information for an existing P-GW service specified as an alphanumeric string of 1 through 63 characters.

statistics { all | name *service_name* **} [verbose]**

Displays P-GW service statistics.
all: Displays statistics for all P-GW services on the system.
name *service_name*: Displays statistics for an existing P-GW service specified as an alphanumeric string of 1 through 63 characters.
If **verbose** is also specified, the information is displayed in more detail.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to view configuration information for P-GW services on this system.

Example

The following command displays service statistics for the P-GW service named *pgw1*:

```
show pgw-service name pgw1
```

show port

Displays information on configured parameters and operational statistics for physical and logical ports in the system.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show port { datalink counters [*slot/port* **] | info [** *slot/port* **] [vlan** *vlan_id* **] | npu counters [** *slot/port* **[tagged | untagged | vlan** *tag_id* **]] | table | utilization table } [| { grep** *grep_options* **| more }]**

---

datalink counters *slot/port*

Displays the information for all data links or only the one specified by the slot/port location of a previously configured port.

---

info [*slot/port* **] [vlan** *vlan_id* **]**

Displays detailed information for all ports within the chassis or only the one specified by slot/port location of a previously configured port.
vlan *vlan_id*: Displays detailed information about all Virtual Local Area Networks (VLANs) in the port/slot. If the optional vlan_id is not specified, this keyword displays port information for all VLANs in the slot/port location.

---

npu counters [*slot/port* **[tagged | untagged | vlan** *tag_id* **]] | bound | unbound]**

Displays the information for Network Processing Unit (NPU) ports. The information for all ports is output or only the one specified by the lsot/port location of a previously configured port.
tagged: Display statistics for all tagged packets.
untagged: Display statistics for all untagged packets.
vlan *tag_id*: Display NPU counters for a previously configured VLAN ID.
bound: Displays individual and cumulative NPU port counters for the bound ports within the current context. If the command is invoked in the local context, all of the bound ports for all contexts and cumulative counter values for all contexts are displayed.
unbound: Displays individual and cumulative NPU port counters for all unbound ports within system.

---

table

Displays information for all physical ports on rear-installed cards with physical interfaces.

---

utilization table

Shows average port utilization in Mbps. The output is a table that lists the current utilization average, a 5-minute average, and a 15-minute average, for all enabled ports.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Display port information for troubleshooting of network communications by viewing statistics and configuration information for physical ports.

Example

The following displays detailed information for port 1 in slot 17:

```
show port info 17/1show port table
```

The following displays information for the data link port 33/1:

```
show port datalink counters 33/1
```

```
show port npu counters 33/1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show power

Displays information about the power on/off status of individual cards and the operating status of installed power filter units.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show power [all | chassis | *card_num* **] [| { grep** *grep_options* **| more }]**

all | chassis | *card_num* **]**

all: Displays power on/off state for all cards in the chassis.
chassis: Displays the operating status of installed power filter units. This is the default setting.
card_num: Displays the power on/off state for a single card specified an integer from 1 through 48.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

View power source information to quickly check the power for all cards within a chassis.

Important: On some platforms, only **show power** is supported with no other keywords or variables.

Example

The following displays power supply status for the chassis:

```
show power
```

The following command displays the power status for all slots:

```
show power all
```

show ppp

Displays the point-to-point protocol (PPP) information, detailed or summarized, for one or all connections by the use of filtering options.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ppp { [counters | full | summary] { all | callid *call_id* **| imsi** *id* **| msid** *ms_id* **| username** *user_name* **} | statistics [pcf-address [** *pcf_ip_addr* **| all] | pdsn-service** *pdsn_name* **] } [| { grep** *grep_options* **| more }]**

counters | full | summary

Filters the output for the level and type of information with the options described below.
counters: Displays PPP statistics.
full: Displays all available information.
summary: Displays only a summary of available information.

all | callid *call_id* **| imsi** *imsi_id* **| msid** *ms_id* **| username** *user_name* **}]**

all: Displays all available information.
callid *call_id*: Displays PPP information only for the call ID specified as a 4-digit hexadecimal number.
imsi *id*: Displays PPP information only for the subscriber with the specified IMSI (International Mobile Subscriber Identity). *id* is a 15-digit field which identifies the subscriber's home country and carrier.
msid *ms_id*: Displays information for a mobile subscriber ID specified as 7 to 16 digits for an IMSI, MIN, or RMI.
username *user_name*: Displays user PPP information for the specified username.

statistics [pcf-address [*pcf_ip_addr* **| all] | pdsn-service** *pdsn_name* **]**

Displays statistics for all packet data services.
pcf-address [*pcf_ip_addr* **| all**] : Displays statistics only for the time the session is connected to the specified PCF (Packet Control Function) or for all PCFs. *pcf_ip_addr* must be specified using IPv4 dotted-decimal notation.
pdsn-service *pdsn_name*: Display statistics only for an existing PDSN service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

View Point-to-Point Protocol information to support troubleshooting subscriber connections by viewing information on PPP connections for a specific subscriber.

Example

The following displays the PPP summary for all connections.

```
show ppp summary all
```

The following outputs the point-to-point detailed information for the user *user1*.

```
show ppp full username user1
```

The following command displays the standard information for the call with ID *FF0E11CD*.

```
show ppp callid ff0e11cd
```

The following command displays the PPP statistics for *pdsn1*.

```
show ppp statistics pdsn-service pdsn1
```

The following command provides summarized information for the PPP statistics.

```
show ppp
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show prepaid 3gpp2

Displays prepaid accounting information for all services or only the service specified.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show prepaid 3gpp2 statistics all [| { grep *grep_options* **| more }]**

show prepaid 3gpp2 statistics { ggsn-service | ha-service | lns-service | pdsn-service { all | name *service_name* **} [| { grep** *grep_options* **| more }]**

show prepaid 3gpp2 statistics per-service-summary } [| { grep *grep_options* **| more }]**

all

Displays prepaid statistics for all services.

ggsn-service

Displays statistics for GGSN service(s).

ha-service

Displays statistics for HA service(s).

lns-service

Displays statistics for LNS service(s).

pdsn-service

Displays statistics for PDSN service(s).

{ all | name *service_name* **}**

all: Displays statistics for all services of the specified type.
name *service_name*: Displays statistics for an existing service specified an alphanumeric string of 1 through 63 characters.

per-service-summary

Displays prepaid statistics per service summary for all services.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Displays Pre-paid statistics for a particular named service or for all services.

Example

To display statistics for a PDSN service named *PDSN1*, enter the following command:

```
show prepaid 3gpp2 statistics pdsn-service name PDSN1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show prepaid wimax

This command displays prepaid WiMAX accounting information for all services or only the service specified.

Product

ASN-GW

Privilege

Inspector

Syntax

show prepaid wimax statistics { all | asngw-service { all | name *service_name* **} | ha-service { all | name** *service_name* **} | per-service-summary } [| { s** *grep_options* **| more }]**

all

This keyword displays prepaid statistics for all services.

asngw-service

Displays prepaid statistics for Access Service Network-Gateway (ASN-GW) service(s).

ha-service

Displays prepaid accounting statistics for Home Agent (HA) service(s).

{ all | name *service_name* **}**

all: Displays statistics for all services of the specified type.
name *service_name*: Displays statistics for an existing service specified as an alphanumeric string of 1 through 63 characters.

per-service-summary

Displays prepaid statistics per service summary for all services.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to display prepaid WiMAX accounting statistics for named service or for all services.

Example

The following command displays prepaid WiMAX accounting statistics for an ASN-GW service named *asn1*:

```
show prepaid wimax statistics asngw-service name asn1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show profile-id-qci-mapping

Displays QoS Class Identifier-Radio Access Network (QCI-RAN) mapping tables configured on this system.

Product

HSGW

Privilege

Inspector

Syntax

show profile-id-qci-mapping table { all | name *table_name* **} [| { grep** *grep_options* **| more }]**

all

Displays information for all QCI-RAN mapping tables configured on this system.

name *table_name*

Displays information for an existing QCI-RAN table specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to display the contents of a specific QCI-RAN mapping table or all mapping tables configured on this system.

Example

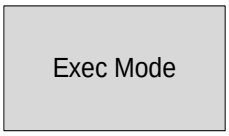
The following command displays the contents of a QCI-RAN mapping table named *table1*:

```
show profile-id-qci-mapping table name table1
```

Chapter 118
Exec Mode Show Commands (Q-S)

This chapter includes the commands **qci-qos-mapping** through **show system uptime**.

The Exec Mode is the initial entry point into the command line interface system. Exec mode **show** commands are useful in troubleshooting and basic system monitoring.



show qci-qos-mapping

Displays QoS Class Identifier-Quality of Service (QCI-QoS) mapping tables configured on this system.

Product

HSGW, P-GW, S-GW

Privilege

Inspector

Syntax

show qci-qos-mapping table { all | name *table_name* } [| { *grep_options* **| more** }]

all

Displays information for all QCI-QoS mapping tables configured on this system.

name *table_name*

Displays information for an existing QCI-QoS mapping table specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display the contents of a specific QCI-QoS mapping table or all mapping tables configured on this system.

Example

The following command displays the contents of a QCI-QoS mapping table named *table1*:

```
show qci-qos-mapping table name table1
```

show qos npu inter-subscriber traffic

Displays configuration information pertaining to Network Processing Unit (NPU) QoS priority queue bandwidth allocation and sharing.

Product

GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show inter-subscriber traffic { bandwidth | bandwidth-sharing }
```

bandwidth

Displays NPU QoS priority queue bandwidth allocation configuration information.

bandwidth-sharing

Displays NPU QoS priority queue bandwidth sharing configuration information.

Usage

Use this command to verify configuration information and for troubleshooting.
When the bandwidth keyword is used, the output is a table showing the configuration status, the priority queue, and the bandwidth allocation per DSCP.
When the bandwidth-sharing keyword is used, the output of is a table displaying the bandwidth sharing configuration per processing card slot/CP number.
For additional information on the NPU QoS functionality, refer to the *System Administration Guide*.

Important: This functionality is not supported for use with the PDSN at this time.

show radius

Displays and statistic information for RADIUS accounting and/or authentication.

Product

PDSN, HA, GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show radius { accounting servers | authentication servers } [detail] [admin-status { enabled | disabled }] [| { grep *grep_options* **| more }] [radius group** *group_name* **[detail] [| { grep** *grep_options* **| more }]]**

accounting servers

Lists information for configured accounting servers and their current state.

authentication servers

Lists information for configured authentication servers and their current state.

[detail]

Displays historical state information for configured servers of the specified type.

admin-status { enabled | disabled }

Displays information for accounting and/or authentication servers with an administrative status of "enabled" or "disabled".

radius group *group_name*

Displays the authentication/authorization RADIUS server group information for an existing server group specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Display the RADIUS server information as part of periodic monitoring of the health of the system.

Example

The following displays the information on configured accounting servers:

```
show radius accounting server
```

The following command displays detailed information for RADIUS accounting servers:

```
show radius accounting servers detail
```

The following command displays detailed information for RADIUS server group *star1* used for authentication:

```
show radius authentication servers radius group star1 detail
```

The following command displays detailed information for RADIUS server group *star1* used for accounting:

```
show radius accounting servers radius group star1 detail
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show radius charging servers

This command displays the RADIUS authentication and accounting servers or server group that are configured for use by charging services.

Product

PDSN, HA, GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show radius charging servers [radius group *group_name* **] [| { grep** *grep_options* **| more }]**

radius group *group_name* **all**

Displays all RADIUS counter information for an existing server group configured for use by charging services. *group_name* is specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information about RADIUS servers or server group configured for use by Charging Services.

Example

The following command displays RADIUS servers configured for Charging Services:

```
show radius charging servers
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show radius client

DIsplays information about the RADIUS client configured on the system.

Product

PDSN, HA, GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show radius client status [| { grep *grep_options* **| more }]**

status

Displays a status summary for the RADIUS client.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Configuring the RADIUS protocol on the system enables RADIUS client functionality. This command is displays information pertaining to the status of the client.

Example

The following command displays detailed information pertaining to the system's RADIUS client:

```
show radius client status
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show radius counters

Displays RADIUS server and statistic information for accounting and/or authentication.

Product

PDSN, HA, GGSN, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show radius counters { all | radius group *group_name* **all | server** *ip_address* **[port** *number* **] | summary [all-contexts [verbose]] } [| { grep** *grep_options* **| more }]**

---

counters { all | server *ip_address* **[port** *number* **] }**

all: Displays statistics for all servers.
server *ip_address*: Displays statistics for the server specified by its IPv4 address.
port *number*: Displays statistics for a port on the server specified as an integer from 0 through 65535.

---

radius group *group_name* **all**

Displays all RADIUS counter information for an existing server group specified as an alphanumeric string of 1 through 63 characters.
all: Displays statistics for all servers.

---

summary [all-contexts [verbose]]

Displays a summary of RADIUS statistics for all the RADIUS servers configured in a specific context.
all-contexts: Displays a summary of RADIUS statistics for all RADIUS servers configured in all context. If **verbose** is also specified, the information is displayed in more detail.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Display the RADIUS server information as part of periodic monitoring of the health of the system.

Example

The following command displays detailed information pertaining to the RADIUS server group *star1* with in current context:

```
show radius counters radius group star1 all
```

The following displays the statistics for the server with IP address *10.2.3.4*, then just port *7777*, followed by **all** services.

```
show radius counters server 10.2.3.4
```

```
show radius counters server 10.2.3.4 port 7777

show radius counters all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show resources

Displays the resource information by CPU or session.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show resources { cpu | npu | session } [ | { grep grep_options | more } ]
```

cpu | npu | session

cpu: Displays resource information by CPU.
npu: Displays resource information by network processing unit (NPU).
session: Displays resource information by session.

| { grep *grep_options* | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View resource utilization as part of troubleshooting systems which appear sluggish or are having excessive connection timeouts or other connection issues.

Example

The following display the resource information by CPU and session, respectively.

```
show resources cpu

show resources session
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show rohc counters

Displays RObust Header Compression (ROHC) counters for all active calls.

Product

PDSN, HSGW, ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show rohc counters [all | callid *call_id* **| imsi** *imsi_num* **| ip-address** *ip_addr* **| msid** *msid_num* **| username** *user_name* **] [| { grep** *grep_options* **| more }]**

all

Displays all information.

callid *call_id*

Displays the information only for the call ID specified as a 4-byte hexadecimal number.

imsi *imsi_num*

Displays information for the specified IMSI (International Mobile Subscriber Identity). The IMSI is an up to 15-digit field which identifies the subscriber's home country and carrier: 3 digits of Mobile Country Code (MCC), 2 or 3 digits of Mobile Network Code (MNC), followed by the Mobile Subscriber Identification Number MSIN. Example: 123-45-678910234. May also be entered as 12345678910234.

ip-address *ip_addr*

Displays information only for the mobile subscriber IP address specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

msid *msid_num*

Displays information only for a mobile subscriber ID from 7 to 16 digits for an IMSI, MIN, or RMI.

username *user_name*

Displays radio-packet (R-P) interface information only for a specified username.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display ROHC counters for all active calls.

Example

The following command displays ROHC counters for all active calls:

```
show rohc counters all
```

show rohc statistics

Displays statistics and counters for RObust Header Compression (ROHC) IP header compression.

Product

PDSN, HSGW, and ASN-GW.

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show rohc statistics [ pdsn-service pdsnsvc_name ] [ asngw-service asngwsvc name ] [
hsgw-service hsgwsvc_name ] [ | { grep grep_options | more } ]
```

Important: Keywords available for this command are license-driven. For example, if a PDSN license is loaded, the **pdsn-service** option is visible.

pdsn-service *pdsnsvc_name*

Displays ROHC statistics and counters for the an existing PDSN service specified as an alphanumeric string of 1 through 63 characters.

asngw-service *asngwsvc_name*

Displays ROHC statistics and counters for an existing ASN-GW service specified as an alphanumeric string of 1 through 63 characters.

hsgw-service *hsgwsvc_name*

Displays ROHC statistics and counters for an existing HSGW service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display ROHC statistics for all services or for a specific ASN-GW, PDSN, or HSGW.

Example

The following command displays ROHC statistics for the PDSN service named pdsn1:

```
show rohc statistics pdsn-service pdsn1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show route-map

Displays entries for all route maps or a specific route map.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show route-map [name *route-map name* **] [| { grep** *grep_options* **| more }]**

name *route-map name*

Displays information for a route-map specified as an alphanumeric string of 1 through 79 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to see the rules configured in all route-maps for the current context.

Example

The following command displays the route-map information for prefix list *Prefix100*:

```
show route-map Prefix100
```

Refer to the **match** and **set** command descriptions in the *Route-map Configuration Mode Commands* chapter for descriptions of the various entries listed.

show rp

Displays radio-packet (R-P) interface statistics using the filtering options specified.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show rp [counters | full | summary] { all | callid *call_id* **| msid** *ms_id* **| peer-address** *peer_ip_address* **| username** *user_name* **} [| { grep** *grep_options* **| more }]**

counters | full | summary

Provides an optional modifier to the output for the desired level and type of information.
counters: Displays R-P protocol statistics.
full: Displays all available information.
summary: Displays only a summary of available information.
These options are not available in conjunction with the keywords **statistics** or **service-option statistics**.

all | callid *call_id* **| msid** *ms_id* **| peer-address** *peer_ip_address* **| username** *user_name*

all: Displays all R-P information.
callid *call_id*: Displays only the information for the call ID specified as a 4-digit hexadecimal number.
msid *ms_id*: Displays information only for a mobile subscriber ID specified by 7 to 16 digits for an IMSI, MIN, or RMI.
peer-address *peer_ip_address*: Displays R-P information for the peer IP address of the PCF specified in IPv4 dotted-decimal notation.
username *user_name*: Displays R-P information for the specified username.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View the R-P interface statistics for the current context.

Example

The following displays the summary for all connections.

```
show rp summary all
```

The following outputs the R-P interface detailed information for the user *isp1user1*.

```
show rp full username isp1user1
```

The following command displays the standard information for the call with ID *FF0E11CD*.

```
show rp callid ff0e11cd
```

The following displays the statistics summary for the R-P facility.

```
show rp
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show rp service-option

Displays the radio-packet (R-P) service option statistics using the filtering options specified.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show rp service-option statistics [number *svc_option_num* **| pdsn-service** *pdsn_name* **] [| { grep** *grep_options* **| more }]**

---

number *svc_option_num* **| pdsn-service** *pdsn_name*

Default: display statistics for all service option numbers and associated packet data services.
number *svc_option_num*: Displays statistics for the specified service option number.
pdsn-service *pdsn_name*: Displays statistics for the specified packet data service.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View the R-P service option statistics for the current context.

Example

The following displays the statistics for all service options.

```
show rp service-option statistics
```

The following displays the statistics for service option *5*.

```
show rp service-option statistics number 5
```

The following command displays the statistics for all service options in collected for the packet data service *sampleService*.

```
show rp service-option statistics pdsn-service sampleService
```

show rp statistics

Displays the radio-packet (R-P) protocol statistics using the filtering options specified.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show rp statistics [ hsgw-service hsgw-name | pcf-summary [  wf1 ] | pdsn-service
pdsn_name | peer-address { peer_address | all } ] [ include-bcmcs ] [ verbose ] [ | {
grep grep_options | more } ]
```

hsgw-service *hsgw_name*

Specifies an eHRPD Serving Gate Way service followed by the name of an HSGW service specified as an alphanumeric string of 1 through 63 characters.

pcf-summary [wf1]

Displays a session summary of Packet Control Function (PCF) statistics.

The **wf1** option displays PCF statistics in wide-format number 1.

pdsn-service *pdsn_name*

Displays the statistics information for the pdsn-service specified as an alphanumeric string of 1 through 63 characters.

peer-address { *peer_address* | all }

- *peer_address*: Displays statistics only for the peer specified by its IP address in IPv4 dotted-decimal notation.
- **all**: Displays statistics for all peers.

verbose

Displays more detailed statistics.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View the R-P statistics for the current context.

Example

The following displays all collected R-P statistics.

```
show rp statistics
```

The following displays the R-P statistics associated with the peer address *10.2.3.4*.

```
show rp statistics peer-address 10.2.3.4
```

The following command displays the R-P statistics for the packet data service *PCFnet*.

```
show rp statistics pdsn-service PCFnet
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show rsvp counters

Displays Resource Reservation Protocol (RSVP) counters using the filtering options specified.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show rsvp counters [all | callid *call_id* **| msid** *ms_id* **| username** *user_name* **]**

all | callid *call_id* **| msid** *ms_id* **| username** *user_name*

all: Displays all RSVP information.
callid *call_id*: Displays information only for the call ID specified as a 4-digit hexadecimal number.
msid *ms_id*: Displays information for a mobile subscriber ID specified a string of 7 to 16 digits for an IMSI, MIN, or RMI.
username *user_name*: Displays RSVP information only for the specified username.

Usage

View the RSVP counters for the current context.

Example

The following displays all collected RSVP counters.

```
show rsvp counters all
```

show rsvp statistics

Displays Resource Reservation Protocol (RSVP) statistics using the filtering options specified.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show rsvp counters [pdsn-service *service* **| sessmgr instance** *instance* **]**

pdsn-service *service* **| sessmgr instance** *instance*

pdsn-service *service*: Displays statistics for the service specified as an alphanumeric string of 1 through 63 characters.
sessmgr instance *instance*: Displays statistics for the specified session manager instance.

Usage

View the RSVP statistics for the current context.

Example

The following displays collected RSVP statistics for a *sampleService*.

```
show rsvp statistics pdsn-service sampleService
```

show sccp-network

Displays SS7 Signaling Connection Control Part (SCCP) network configuration and status information.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show sccp-network { *ntwk_index* | all } [status [all | dpc]]

ntwk_index

Displays configuration and status information for the SSCP network configuration with the network index specified as an integer from 1 through 12.

all

Displays all available configuration and status information for all SSCP networks.

status all

Displays all status information for specified SCCP networks.

status dpc

Displays status information for the device in the SCCP network identified by the destination point-code (DPC).

Usage

Use this command to display global SCCP statistics or to display SCCP statistics for a specified service or network.

Example

The following command displays global SCCP statistics:

```
show sccp-network all
```

The following command displays information for an SCCP network configuration with the network index of *1*:

```
show sccp-network 1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show sccp statistics

Displays SS7 Signaling Connection Control Part (SCCP) statistics for services that use the SCCP protocol.

Product

SGSN

Privilege

Inspector

Syntax

show sccp statistics [iups-service *iups_srvc_name* **| map-service** *map_srvc_name* **| sccp-network** *ntwk_index* **[dpc** *dpc* **[ssn** *ssn* **] | global-title-translation { address-map instance** *add_map_inst* **| association instance** *assoc_inst* **} [sessmgr instance** *sessmgr_inst* **]] [| { grep** *grep_options* **| more }]**

iups-service *iups_srvc_name*

Displays SCCP protocol statistics for an existing IuPS service in the current context specified as an alphanumeric string of 1 through 63 characters.

map-service *map_srvc_name*

Displays SCCP protocol statistics for the an existing Mobile Application Part (MAP) service in the current context specified as an alphanumeric string of 1 through 63 characters.

sccp-network *ntwk_index*

Displays SCCP protocol statistics for the SSCP network configuration with a network index specified as an integer from 1 through 12.
The following filters can be added to fine tune the display of SCCP network statistics:

- **dpc** *dpc*: Enter a standard pointcode address to limit the display of SCCP network statistics to those for the identified DPC.
- **ssn** *ssn*: Enter an integer from 1 to 255 to limit the display of SCCP network statistics to those for the identified subsystem number.
- **global-title-translation address-map instance** *add_map_inst*: Enter an integer from 1 to 4096 to limit the display of SCCP network statistics to those for the identified GTT address-map.
- **global-title-translation association instance** *assoc_inst*: Enter an integer from 1 to 16 to limit the display of SCCP network statistics to those for the identified GTT association.
- **sessmgr instance** *sessmgr_inst*: Enter an integer from 1 to 384 to limit the display of SCCP network statistics to those for the identified session manager.

Usage

Use this command to display global SCCP statistics or to display SCCP statistics for a specified service or SCCP network.

Example

The following command displays global SCCP statistics:

```
show sccp statistics
```

The following command displays SCCP statistics for the IuPS service named *iups-serv1*:

```
show sccp statistics iups-service iups-serv1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show sctp-param-template

Displays configuration information for Stream Control Transmission Protocol (SCTP) parameter templates configured on this system.

Product

MME

Privilege

Inspector

Syntax

show sctp-param-template { all | name *template_name* **} [| { grep** *grep_options* **| more }]**

all

Displays configuration information for all SCTP parameter templates configured on this system.

name *template_name*

Displays configuration information for an existing SCTP parameter template specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view configuration information for SCTP parameter templates on this system.

Example

The following command displays configured parameters for an SCTP parameter template named *sctp_pt3*:

```
show sctp-param-template name sctp_pt3
```

show session counters historical

Displays historical information for session-related counters based on data collected in bulk statistics.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show session counters historical { all | arrived | callops | connected | disconnected |
failed | handoff | rejected | renewal } [ all-intervals | cumulative | graph |
incremental | recent-intervals | table ]
```

all

Displays data for all counters either as a single, wide table or multiple graphs.

arrived

Displays only data for “total calls arrived” counters. This is based on the “sess-ttlarrived” statistic in the system schema.

callops

Displays data for all call operations. This is a calculated value based on the following formula:
(arrived + rejected + disconnected + failed + handoffs + renewals)

connected

Displays only data for “total calls connected” counters. This is based on the “sess-ttlconnected” statistic in the system schema.

disconnected

Displays only data for “total calls disconnected” counters. This is based on the “sess-ttldisconn” statistic in the system schema.

failed

Displays only data for “total calls failed” counters. This is based on the “sess-ttlfailed” statistic in the system schema.

handoff

Displays only data for “total handoffs” counters. This is based on the “sess-ttlhandoff” statistic in the system schema.

rejected

Displays only data for “total calls rejected” counters. This is based on the “sess-ttlrejected” statistic in the system schema.

renewal

Displays only data for "total renewal" counters. This is based on the "sess-ttlrenewal" statistic in the system schema.

Output Options

The following output options are available for this command:

- **all-intervals**Displays all available historical information from all samples. This this filter is used by default.
- **cumulative**Displays total data for all samples up to and including the last one. In this view, values increase over time.
- **graph**Displays data in graphical form.
- **incremental**Displays data changes for each specific sample. The data for each sample is the amount of change since the previous sample. This filter is used by default.
- **recent-intervals**Displays historical information for only recent samples.
- **table**Displays data in tabular form. This is the default view.

Usage

This command provides the ability to track key session-related statistic information over time. This information can be used as part of system performance monitoring and capacity planning.

Important: The information provided in the output of this command requires that bulk statistics functionary be enabled on the system. Refer to the *System Administration Guide* for more information on configuring and enabling bulk statistics support.

The output of this command displays historical data collected at various sample intervals. The interval length is 15 minutes and is not user-configurable. Up to 192 samples (two days' worth of data) are maintained.

Important: Data collection is "best-effort" over these intervals. Data is preserved on system management card switchovers. As with all counters, certain session failures can cause inaccuracies with counters, including counters which appear to go backwards.

Each sample is identified by a timestamp that displays the approximate time the data was gathered. the timestamp is in the format YYYY:MM:DD:hh:mm:ss.
Data acquired during the sample may be marked with an "S" appended to the end of the timestamp or to the counter value. The "S" indicates that the data is suspect (potentially bad). Occurrences of this result from events like changes to the real time clock, which can cause an interval to be an atypical length. Instances of suspect data should be rare. Additionally, there may be occasions in which a sample may be marked as "invalid". "invalid" identifies bad data, a situation that could result when the polling has not run long enough, or because of an unexpected error retrieving data.
Since baseline values must be obtained prior to collecting interval samples, the first interval of data will not be available until up to twice the interval period.

Example

The following command displays cumulative total calls arrived information for the most recent intervals and displays the output in graphical format:

```
show session counters historical arrived recent-intervals cummulative
graph
```

The following command displays historical data for all counters for all intervals and displays the output in tabular format:

```
show session counters historical all
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show session counters pcf-summary

Displays the Packet Control Function (PCF) summary which include the number of calls, call types, and Tx/Rx packets/octets statistics.

Product

PDSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show session counters pcf-summary [call-types | data | wf1 [pcf *pcf_address* **| [| { grep** *grep_options* **| more }]]]**

call-types

Displays the number of calls and the types of calls.

data

Displays the number of successful calls and Tx/Rx packets/octets statistics.

pcf *pcf_address*

Displays the given PCF summary for a particular address.

wf1

Displays the PCF summary in a single very wide line.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display a summary of all PCFs.

Example

```
show session counters pcf-summary
```

show session disconnect-reasons

Displays a list of the reasons for call disconnects and the number of calls disconnected for each reason.

Product

All

Privilege

Security Administrator, Administrator, Inspector, Operator

Syntax

show session disconnect-reasons [gprs-only | sgsn-only | mme-only | verbose] [| { grep *grep_options* **| more }]]**

gprs-only

Only supported on the SGSN.
This keyword limits the display to session disconnect reasons for the SGSN's 2G MM and PDP context disconnects.

sgsn-only

Only supported on the SGSN.
Displays session disconnect reasons for the SGSN's 3G MM and PDP context disconnects.

mme-only

Displays session disconnect reasons for MME call disconnects.

verbose

List all disconnect reasons even if the values are zero (0).

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display a list of the reasons why calls were disconnected.

Example

To view session disconnect statistics, enter the following command:

```
show session disconnect-reasons
```

To view a list of the disconnect reasons with verbose output, enter the following command:

```
show session disconnect-reasons verbose
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show session duration

Displays session duration information for the current context filtered by the options specified.

Product

All

Privilege

Security Administrator, Administrator, Inspector, Operator

Syntax

show session duration [*session_filter* **] [| { grep** *grep_options* **| more }]**

session_filter

Specifies the name of the entity whose session duration information is to be filtered and displayed. This options are:

- **asn-peer-address** *ip_address*: Displays session information for the ASN GW peer whose IP address is specified in IPv4 dotted-decimal notation.
- **asngw-service** *service_name*: Displays session information for the specified ASN-GW service.
- **asnpc-peer-address** *ip_address*: Displays session information for the Access Service Network Paging Controller (ASN PC) peer whose IP address is specified in IPv4 dotted-decimal notation.
- **asnpc-service** *service_name*: Displays session information for the specified ASN PC service.
- **apn** *apn_name*: Displays session information for an existing Access Point Name (APN) specified as an alphanumeric string of 1 through 63 characters that is case sensitive.
- **cscf-service** *service_name*:Displays session information for an existing Call Session Control Function (CSCF) service specified as an alphanumeric string of 1 through 63 characters.

Important: Displays information for in-progress CSCF SIP calls only. Registrations are not considered calls.

- **dhcp-server** *dhcp_address*: Displays session information for the Dynamic Host Configuration Protocol (DHCP) server specified by its IP address in IPv4 dotted-decimal notation.
- **fa** *fa_address*: Displays session information for the foreign agent (FA) whose IP address is specified in IPv4 dotted-decimal notation.
- **fa-service** *fa_name*: Displays session information for the named foreign agent service.
- **ggsn-service** *ggsn_name*: Displays session information for an existing GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.
- **gprs-only**: Limits the display to the session information for the SGSN's 2G MM and PDP contexts.
- **ha** *ha_address*: Displays session information for the home agent specified by its IP address in IPv4 dotted-decimal notation.
- **ha-service** *ha_name*: Displays session information for the named home agent (HA) service.
- **hnbgw-only**: Displays session information for the HNB-GW service related sessions instances (such as HNB, IuPS, IuCS).
- **hsgw-service** *service_name*: Displays session information for an existing HSGW service specified as an alphanumeric string of 1 through 63 characters.

- **lma-service** *service_name*: Displays session information for an existing Local Mobility Anchor (LMA) service specified as an alphanumeric string of 1 through 63 characters.
- **mme-service** *service_name*: Displays session information for an existing Mobility Management Entity (MME) service specified as an alphanumeric string of 1 through 63 characters.
- **mag-service** *service_name*: Displays session information for an existing Mobile Access Gateway (MAG) service specified as an alphanumeric string of 1 through 63 characters.
- **pcf** *pcf_address*: Displays session information for the packet control function specified by its IP address in IPv4 dotted-decimal notation.
- **pdsn-service** *pdsn_name*:Displays session information for the named packet data service.

Important: If no PCF address or PDSN service is specified, the session information for all sessions is displayed.

- **sgsn-address** *sgsn-address*: Displays session information for the SGSN specified by its IP address in IPv4 dotted-decimal notation.
- **sgsn-only**: Limits the display to the session information for the SGSN's 3G MM and PDP contexts.
- **sgw-service** *service_name*: Displays session information for an existing S-GW service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View the session information to troubleshoot subscriber problems and for general monitoring for orphaned sessions.

Example

The following commands display the duration for the session connected to the packet control function with address *10.2.3.4*, packet data service *sampleService*, and for all sessions, respectively.

```
show session duration pcf 10.2.3.4

show session duration pdsn-service sampleService

show session duration
```

show session-event-record

Displays session event module statistics and file space usage information.

Product

S-GW

Privilege

Operator

Syntax

```
show session-event-record { file-space-usage | statistics }
```

file-space-usage

Displays session event module file storage limits and capacities.

statistics

Displays session event module statistics regarding the handling and transfer of event records to an external collection server.

Usage

View the session event information to troubleshoot handling and transfer problems and for general monitoring for file storage use.

Example

The following command displays the file storage limit and use for all event modules on the system:

```
show session-event-record file-space-usage
```

show session progress

Displays session progress information for the current context filtered by the options specified.

Product

All

Privilege

Security Administrator, Administrator, Inspector, Operator

Syntax

show session progress [asn-peer-address *ip_address* **| asngw-service** *service_name* **| asnpc-service** *service_name* **| asnpc-peer-address** *ip_address* **| apn** *apn_name* **| cscf-service** *service_name* **| dhcp-server** *dhcp_address* **| fa** *fa_address* **| fa-service** *fa_name* **| ggsn-service** *ggsn_name* **| ha** *ha_adress* **| ha-service** *ha_name* **| hsgw-servie** *service_name* **| lma-service** *service_name* **| mag-service** *service_name* **| mme-address** *mme_address* **| mseg-service** *mseg_service_name* **| pcf { ** *pcf_address* **| all } | pdsn-service** *pdsn_name* **| pdsnclosedrp-service | pgw-address** *ip_address* **| sgsn-address** *sgsn_address* **| sgw-service** *service_name* **] [| { grep** *grep_options* **| more }]**

---

progress [asn-peer-address *ip_address* **| asngw-service** *service_name* **| asnpc-service** *service_name* **| asnpc-peer-address** *ip_address* **| apn** *apn_name* **| cscf-service** *service_name* **| dhcp-server** *dhcp_address* **| fa** *fa_address* **| fa-service** *fa_name* **| ggsn-service** *ggsn_name* **| ha** *ha_adress* **| ha-service** *ha_name* **| hsgw-servie** *service_name* **| lma-service** *service_name* **| mag-service** *service_name* **| mme-address** *mme_address* **| mseg-service** *mseg_service_name***| pcf { ** *pcf_address* **| all } | pdsn-service** *pdsn_name* **| pdsnclosedrp-service | pgw-address** *ip_address* **| sgsn-address** *sgsn_address* **| sgw-service** *service_name* **]**

progress: indicates session progress information is to be displayed.

- **asn-peer-address** *ip_address*: Displays session information for the Access Service network-Gateway (ASN-GW) peer specified by its IP address in IPv4 dotted-decimal notation.
- **asngw-service** *service_name*: Displays session information for the named ASN-GW service.
- **asnpc-service** *service_name*: Displays session information for the named Access Service Network Paging Controller (ASN PC) service.
- **asnpc-peer-address** *ip_address*: Displays session information for the ASN PC peer specified by its IP address in iIPv4 dotted-decimal notation.
- **apn** *apn_name*: Displays session information for an existing Access Point Name (APN) specified as an alphanumeric string of 1 through 63 characters that is case sensitive.
- **cscf-service** *service_name*: Displays session information for an existing Call Session Control Function (CSCF) service specified as an alphanumeric string of 1 through 63 characters.

Important: Displays information for in-progress CSCF SIP calls only. Registrations are not considered calls.

- **dhcp-server** *dhcp_address*: Displays session information for the Dynamic Host Configuration Protocol (DHCP) server specified by its IP address in IPv4 dotted-decimal notation.
- **fa** *fa_address*: Displays session information for the foreign agent (FA) whose IP address is specified in IPv4 dotted-decimal notation.

- **fa-service** *fa_name*: Displays session information for the named foreign agent service.
- **ggsn-service** *ggsn_name*: Displays session information for an existing GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.
- **gprs-only**: Limits the display to the session information for the SGSN's 2G MM and PDP contexts.
- **ha** *ha_address*: Displays session information for the home agent specified by its IP address in IPv4 dotted-decimal notation.
- **ha-service** *ha_name*: Displays session information for the named home agent (HA) service.
- **hnbgw-only**: Displays session information for the HNB-GW service related sessions instances (such as HNB, IuPS, IuCS).
- **hsgw-service** *service_name*: Displays session information for an existing HSGW service specified as an alphanumeric string of 1 through 63 characters.
- **lma-service** *service_name*: Displays session information for an existing Local Mobility Anchor (LMA) service specified as an alphanumeric string of 1 through 63 characters.
- **mme-service** *service_name*: Displays session information for an existing Mobility Management Entity (MME) service specified as an alphanumeric string of 1 through 63 characters.
- **mag-service** *service_name*: Displays session information for an existing Mobile Access Gateway (MAG) service specified as an alphanumeric string of 1 through 63 characters.
- **pcf** *pcf_address*: Displays session information for the packet control function specified by its IP address in IPv4 dotted-decimal notation.
- **pdsn-service** *pdsn_name*:Displays session information for the named packet data service.

Important: If no PCF address or PDSN service is specified, the session information for all sessions is displayed.

- **pgw-address** *ip_address*: Displays session progress information for the P-GW specified by its IP address in IPv4 dotted-decimal notation.
- **sgsn-address** *sgsn-address*: Displays session information for the SGSN specified by its IP address in IPv4 dotted-decimal notation.
- **sgw-service** *service_name*: Displays session progress information for an existing S-GW service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View the session information to troubleshooting subscriber problems and for general monitoring for orphaned sessions.

Example

The following commands display the status information for the session connected to the packet control function with address *10.2.3.4*, packet data service *sampleService*, and for all sessions, respectively.

```
show session progress pcf 10.2.3.4
```

```
show session progress pdsn-service sampleService

show session progress
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show session recovery status

Displays session recovery status information for the current context filtered by the options specified.

Product

All

Privilege

Security Administrator, Administrator, Inspector, Operator

Syntax

show session recovery status [verbose] [| { grep *grep_options* **| more }]**

recovery status

Displays the current status of the system's ability to recover from a hardware or software fault that requires the recovery of home agent-based Mobile IP session(s).

verbose

Includes per-CPU Session Recovery status.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View the session information for troubleshooting subscriber problems and for general monitoring for orphaned sessions.

Example

To display the session recovery status information, enter the following command:

```
show session recovery status
```

Adding the optional verbose keyword to this command provides more details.

```
show session recovery status verbose
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show session setuptime

Displays session setup time information for all sessions or sessions associated with the specified Access Gateway (AGW).

Product

PDSN, HNB-GW, SGSN

Privilege

Operator

Syntax

show session setuptime [hnbgw-only | pcf *pcf_address* **| gprs-only | sgsn-address** *sgsn_address***| sgsn-only] [| { grep** *grep_options* **| more }]**

[hnbgw-only | mme-only | pcf pcf_address | gprs-only | sgsn-address *sgsn_address* **| sgsn-only]**

Displays the call setup times aggregated into basic ranges of time.

- **hnbgw-only**: Filters and displays the call setup information for HNB-GW calls only.
- **pcf** *pcf_address*: displays call setup data for the packet control function whose IP address is specified as *pcf_address*. *pcf_address* must be specified using IPv4 dotted-decimal notation. The call setup times for all PCFs is displayed when no specified PCF is specified.
- **gprs-only**: Displays 2G call setup data for the for the SGSN for the MM and PDP contexts.
- **sgsn-address** *sgsn_address***:** Displays call setup times for the specified SGSN. *sgsn_address* is the IP address of the SGSN and must be expressed in IPv4 dotted-decimal notation. This keyword is used by the GGSN.
- **sgsn-only**: Displays 3G call setup data for the for the SGSN for the MM and PDP contexts.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View the session information to troubleshooting subscriber problems and for general monitoring for orphaned sessions.
When no keywords are specified, the information shown is cumulative for all sessions that have been facilitated by the system.

Example

The following command shows setup time statistics for all sessions from the PCF at IP address *192.168.10.3*:

```
show session setuptime pcf 192.168.10.3
```

show session subsystem

Displays session information for system subsystems. If no keywords are specified, information for all subsystems is displayed.

Product

All

Privilege

Security Administrator, Administrator, Inspector, Operator

Syntax

show session subsystem [full | facility *facility* **[all | instance** *id* **]] [verbose] [| { grep** *grep_options* **| more }]**

[full | facility *facility* **[all | instance** *id* **]]**

- **full**: Indicates that a full statistics summary of all subsystems is to be displayed.
- **facility** *facility*: Specifies the facility for which subsystem statistics is to be displayed where *facility* is specified as one of:
  - **a11mgr**: A11 Manager
  - **aaamgr**: Accounting and Authentication Manager
  - **aaaproxy**: AAA Proxy Manager
  - **asngwmgr**: ASN Gateway Manager
  - **asnpcmgr**: ASN Paging/Location-Registry Manager
  - **cscfmgr**: SIP CSCF Manager
  - **dgmbmgr**: Diameter Gmb Application Manager
  - **diamproxy**: Diameter Proxy Application Manager
  - **egtpegmgr**: EGTP Egress Demux Manager
  - **egtpinmgr**: EGTP Ingress Demux Manager
  - **famgr**: Foreign Agent Manager
  - **gtpumgr**: GTPUMGR Demux Manager
  - **gtpcmgr**: GTPC Manager
  - **hamgr**: Home Agent Manager
  - **hnbmgr**: HNBGW HNB Manager
  - **imsimgr**: SGSN IMSI Manager
  - **ipsgmgr**: IP Services Gateway Manager
  - **l2tpdemux**: L2TP Demux Manager
  - **l2tpmgr**: L2TP Manager
  - **linkmgr**: SGSN/SS7 Master Manager
  - **magmgr**: Mobile Access Gateway Manager
  - **megadiammgr**: Mega Diameter Manager

- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager logging facility
- **mmgr**: SGSN/SS7 Master Manager
- **phsgwmgr**: PHS Gateway Manager
- **phspcmgr**: PHS Paging Controller Manager
- **sessmgr**: Session Manager
- **sgtpcmgr**: SGSN GTPC Manager

- **all | instance** *id*: the keyword **all** indicates all instances of the specified facility are to be displayed whereas the keyword **instance** specifies a specific instance for which information is to be displayed where *id* must be specified as an integer from 0 through 4294967295. If all or instance is not specified summary statistics are displayed.

verbose

Displays everything the **show session subsystem** command displays with the exception that the Setup Time statistics are reported in 100 millisecond increments from 100 ms up to 9600 ms.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

View the session information to troubleshooting subscriber problems and for general monitoring for orphaned sessions.
If this command is entered with no keywords, the information displayed is cumulative for all sessions facilitated by the system.

Example

The following commands display the statistics information summarized for all sessions, then for the *famgr* facility (all sessions), and finally only for the session ID *127589* for the *hamgr* subsystem.

```
show session subsystem full

show session subsystem facility famgr all

show session subsystem facility hamgr instance 127589
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show session trace

Displays status and statistics for the session trace application.

Product

GGSN, MME, P-GW, S-GW

Privilege

Inspector

Syntax

show session trace { statistics | subscriber network-element { ggsn | mme | pgw | sgw } trace-ref *value* **| tce-address** *ip_address* **tce-index** *num* **| tce-summary | trace-summary } [| { grep** *grep_options* **| more }]**

statistics

Displays summary statistics for the session trace subsystem.

subscriber network-element { ggsn | mme | pgw | sgw } trace-ref *value*

Displays status and statistics for a specified session trace using the network element type; GGSN, MME, P-GW, and S-GW, and a valid trace reference of 12 characters.

tce-address *ip_address* **tce-index** *num*

Displays status and statistics for an existing Trace Collection Entity (TCE) connection specified by its IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.
tce-index *num*: Specifies a TCE index of the trace collection entity as an integer from 0 through 7.

tce-summary

Displays a summary of all active TCE connections.

trace-summary

Displays a summary of all active session traces.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display status and statistics for the session trace application.

Example

The following command displays status and statistics for a subscriber session trace on a P-GW with a trace reference of *32223398765*:

```
show session trace subscriber network-element pgw trace-ref 32223398765
```

The following command displays status and statistics for a subscriber session trace on an MME with a trace reference of *32221234567*:

```
show session trace subscriber network-element mme trace-ref 32223398765
```

The following command displays status and statistics for a subscriber session trace on an GGSN with a trace reference of *1203398765*:

```
show session trace subscriber network-element ggsn trace-ref 1203398765
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show sgs-service

Displays information and statistics about Visitor Location Register (VLR) SGs interface services configured on this system.

Product

MME

Privilege

Inspector

Syntax

show sgs-service { all | name *name* **| statistics { all | name** *name* **} | vlr-status [service-name** *name* **] [vlr-name** *name* **] [full]**

all

Displays information about all SGs interface services configured on this system.

---

name *name*

Displays information about an existing SGs service specified as an alphanumeric string of 1 through 63 characters.

---

statistics { all | name *name* **}**

Displays statistics for SGs services configured on this system.
all: Displays statistics for all SGs services configured on this system.
name *name*: Displays statistics for an existing SGs service specified as an alphanumeric string of 1 through 63 characters.

---

vlr-status [service-name *name* **] [vlr-name** *name* **] [full]**

Displays status information about VLRs configured in SGs services on this system.
service-name *name*: Displays names and states of VLRs configured in an existing SGs service specified as an alphanumeric string of 1 through 63 characters.
vlr-name *name*: Displays the name and state of an existing VLR configured in SGs services on this system and specified as an alphanumeric string of 1 through 63 characters.
full: Displays additional information about VLRs configured in SGs services on this system. Additional information includes ports, addresses and peer IDs.

Usage

Use this command to display information and statistics about SGs services configured on this system.

Example

The following command displays statistics for an SGs service named *sgs3*:

```
show sgs-service name sgs3
```

The following command displays VLR status information for a configured VLR named *vlr-main*:

```
show sgs-service vlr-status vlr-name vlr-main
```

show sgsn-operator-policy

This command has been deprecated. Refer to the **show operator-policy** command.

show sgsn

Displays session manager (SessMGR) statistics specific to the SGSN service.

Product

SGSN

Privilege

Inspector

Syntax

show sgsn sessmgr { all | instance *smgr_inst* **}**

all

Displays all SessMGR statistics specific to the system's SGSN services.

instance *smgr_inst*

Displays the statistics for a session manager instance of the SGSN service specified as an integer between 1 and 10000000.

Usage

Use this command to display information for SGSN services.

Example

The following command displays SGSN SessMGR statistics for all SGSN services on the system:

```
show sgsn sessmgr all
```

show sgsn-fast-path

Displays information related to SGSN fast-path.

Product

SGSN

Privilege

Inspector

Syntax

```
show sgsn-fast-path statistics [ all | smgr-instance smgr_inst ] [ | { grep grep_options
| more } ]
```

all

Displays fast-path statistics for all session managers.

smgr-instance *smgr_inst*

Displays the fast-path statistics for a session manager instance specified as an integer between 1 and 65535.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display statistics for SGSN fast-path configurations.

Example

The following command displays fast-path statistics for all SGSN session managers:

```
show sgsn sessmgr all
```

show sgsn-map-app

Displays collected statistics for the SGSN Mobile Application Part (MAP).

Product

SGSN

Privilege

Inspector

Syntax

show sgsn-map-app statistics [| { grep *grep_options* **| more }]**

all

Displays collected statistics for the SGSN MAP application.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display statistics for the SGSN MAP application.

Example

The following command displays SGSN MAP statistics:

```
show sgsn-map-app statistics
```

show sgsn-mode

Displays the SGSN global configuration.

Product

SGSN

Privilege

Inspector

Syntax

show sgsn-mode[| { grep *grep_options* **| more }]**

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display the configuration created with the commands in the SGSN Global Configuration mode.

Example

The following command displays the SGSN global configuration:

```
show sgsn-mode
```

show sgsn-pool

Displays collected pooling statistics for either GPRS services or SGSN services.

Product

SGSN

Privilege

Inspector

Syntax

show sgsn-pool statistics { gprs-service *srvc_name* **| sgsn-service** *srvc_name***} { nri-value** *nri_value* **| peer-non-broadcast-lac** *lac* **rac** *rac* **| target-load-in-progress [smgr-instance** *smgr_instance* **| target-nri** *target_nri* **] | target-offloaded-to-peer [target-nri** *target_nri* **] } [| { grep** *grep_options* **| more }]**

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display the collected statistics for pooling in either GPRS or SGSN services. The outputs can be filtered to focus the statistics displayed.

Example

The following command displays the:

```
show sgsn-pool statistics sgsn-service sgsn1 nri-value 3
```

show sgsn-service

Displays information about the configured SGSN services in the current context.

Product

SGSN

Privilege

Inspector

Syntax

show sgsn-servie { all | name *srvc_name* **}**

all

Displays information for all SGSN services in the current context.

name *srvc_name*

Displays information for an existing SGSN service specified as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to display information for SGSN services.

Example

The following command displays information for all SGSN services in the current context:

```
show sgsn-service all
```

The following command displays information for an SGSN service in the current context that is named *sgsn1*:

```
show sgsn-service name sgsn1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show sgtp-service

Displays information about the configured GPRS Tunnelling Protocol (SGTP) services in the current context, including GTP-C and GTP-U operational configuration.

Product

SGSN, PDG/TTG, MME

Privilege

Inspector

Syntax

show sgtp-service { all [gtpu-table] | ggsn-table [smgr-instance *smgr_instance* **] | mbms-bearers | name** *srvc_name* **[gtpu-table] | sgsn-table }**

all [gtpu-table]

Displays configuration information for all of the SGTP services defined for the current context.
gtpu-table: Limits the output to GTPU information for all SGTP services.

ggsn-table [smgr-instance *srvc_name* **]**

Displays GGSN information configured for the SGTP service(s) in the current context.
smgr-instance *srvc_name* enter an integer from 1 through 384 to limit the GGSN output to information for a specific session manager.

mbms-bearers

This keyword is specific to the SGSN and is not yet supported.

name *srvc_name* **[gtpu-table]**

Displays information for the specified SGTP service in the current context. *srvc_name* must be an alphanumeric string of 1 through 63 characters that identifies a configured SGTP service.
gtpu-table: Limits the output to GTPU information for a specific SGTP service.

sgsn-table

Displays SGSN information configured for the SGTP service(s) in the current context.

Usage

Use this command to control the display of SGTP services information.

Example

The following command displays information for all SGTP services in the current context:

```
show sgtp-service all
```

The following command displays the GGSN information in SGTP services in the current context:

```
show sgtp-service ggsn-table
```

The following command displays the SGSN information in SGTP services in the current context:

show sgtp-service sgsn-table

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show sgtpc statistics

Displays all statistics, for SGSN GPRS Tunnelling Protocol (SGTP) interface parameters, collected since the last restart or last use of a **clear** command.

Product

SGSN, PDG/TTG, MME

Privilege

Inspector

Syntax

show sgtpc statistics [all | gsn-address *ipv4_address* **| sgtp-service** *sgtp_srvc_name* **] [verbose][| { grep** *grep_options* **| more }]**

all

Displays configuration information for all of the SGTP services defined for the current context.

gsn-address *ipv4_address*

Displays statistics for an SGSN specified by its IP address in IPv4 dotted-decimal notation. This must be an existing and active interface.

sgtp-service *sgtp_srvc_name*

Displays statistics for an existing SGTP service specified as an alphanumeric string from 1 through 63 characters.

verbose

Causes the system to displays more detailed level of statistics.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information for SGSN services.

Example

The following command displays statistics for the SGTP service named *sgtp1*:

```
show sgtpc statistics sgtp-service sgtp1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show sgtpu statistics

Displays all transmission and reception statistics for pre-defined and active GTP-U interfaces collected since the last restart or last use of a **clear** command.

Product

SGSN, PDG/TTG

Privilege

Inspector

Syntax

show sgtpu statistics [ggsn-address *ipv4_address* **| gprs-service** *gprs_srvc_name* **nsei** *nse_id* **| iups-bind-address** *ipv4_address*| **iups-service** *iups_srvc_name* **| rnc-address** *ipv4_address* **| sgtp-service** *sgtp_srvc_name* **][| { grep** *grep_options* **| more }]**

ggsn-address *ipv4_address*

Displays statistics for the GGSN specified by its IP address in IPv4 dotted-decimal notation.

gprs-service *gprs_srvc_name* **nsei** *nse_id*

Displays NSEI-based GTPU statistics associated with an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.
nsei *nse_id*: Specifies a GPRS NSEI as an integer from 0 through 65535.

iups-bind-address *ipv4_address*

Displays SGSN GPRS Tunnelling Protocol (SGTP) statistics for an Iu GTPU interface specified by its IP address in IPv4 dotted-decimal notation.

iups-service *iups_srvc_name*

Displays statistics for an existing IuPS service specified as an alphanumeric string of 1 through 63 characters.

rnc-address *ipv4_address*

Displays statistics for a Radio Network Controller (RNC) identified by its IP address in IPv4 dotted-decimal notation.

sgtp-service *sgtp_srvc_name*

Displays statistics for an existing SGTP service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display statistics for the SGTPU interface.

Example

The following command displays GPTP-U statistics for the traffic between an SGSN and a connected RNC:

```
show sgtpu statistics rnc-address 123.1.2.3
```

show sgw-service

Displays configuration settings and/or service statistics for Serving Gateway (S-GW) services on this system.

Product

S-GW

Privilege

Inspector

Syntax

show sgw-service { all | name *service_name* **| statistics { all | name** *service_name* **} } [| { grep** *grep_options* **| more }]**

---

all

Displays configuration information for all S-GW services configured on this system.

---

name *service_name*

Displays configuration information for an existing S-GW service c specified as an alphanumeric string of 1 through 63 characters.

---

statistics { all | name *service_name* **}**

all: Displays statistics for all S-GW services on this system or for a specified service.
name *service_name*: Displays statistics for an existing S-GW service specified as an alphanumeric string of 1 through 63 characters.

| { grep *grep_options* **| more }**

Indicates the output of the command is to be piped (sent) to the command specified.
A command to send output to must be specified.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

Usage

Use this command to view configuration settings and/or service statistics for S-GW services on this system.

Example

The following command displays service statistics for the S-GW service named *sgw1*:

```
show sgw-service statistics name sgw1
```

show sms statistics

Displays traffic statistics for the Short Message Service (SMS).

Product

SGSN

Privilege

Inspector

Syntax

show sms statistics [gprs-only | sgsn-only] [name *map_srvc* **] [verbose] [| { grep** *grep_options* **| more }]**

gprs-only

Displays only GPRS access type SMS statistics.

sgsn-only

Displays only UMTS access type SMS statistics.

name *map_srvc*

Displays statistics for an existing MAP service specified as an alphanumeric string of 1 through 63 characters.

verbose

Causes the system to displays more detailed level of statistics.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display traffic statistics for the SMS services.

Example

Use the following command to display SMS statistics for 3G traffic:

```
show sms statistics sgsn-only
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show sndcp statistics

Displays statistics for the packet traffic going through the Subnetwork Dependent Convergence Protocol (SNDCP) layer.

Product

SGSN

Privilege

Inspector

Syntax

show sndcp statistics [gprs-service *srvc_name* **] [verbose] [| { grep** *grep_options* **| more }]**

gprs-service *srvc_name*

Displays statistics for an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

verbose

Displays a more detailed level of statistics.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display SNDCP traffic statistics. Include the **gprs-service** keyword to filter the output to statistics for only one GPRS service.

Example

Use the following command to display all SNDCP layer traffic statistics:

```
show sndcp statistics verbose
```

Use the following command to display SNDCP layer traffic statistics for the *test1* GPRS service:

```
show sndcp statistics gprs-service test1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show snmp

Displays information on the Simple Network Management Protocol (SNMP) servers and interfaces.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show snmp { accesses | communities | contexts | notifies | server | transports | trap [history | statistics { verbose } { wide }] | views } [| { grep *grep_options* **| more }]**

---

accesses

Displays SNMP server usage statistics.

---

communities

Displays SNMP community strings.

---

contexts

Displays SNMP information per context.

---

notifies

Displays SNMP event trap and notification statistics.

---

server

Displays SNMP server configuration information.

---

transports

Displays trap destination configuration information.

---

trap [history | statistics { verbose } { wide }]

history: Displays SNMP event trap history. **trap history** Displays up to 5,000 time-stamped trap records stored in a buffer. The buffer may be cleared by entering the **clear snmp history** command.
statistics: Displays SNMP event trap and notification statistics.
verbose: Displays rows for every defined trap, even if never generated.
wide: Displays trap statistics data in excess of 80 columns.

---

views

Displays SNMP views.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Display SNMP information as part of system verification and troubleshooting.

Example

The following commands display the usage statistics, community string information, event trap and notification data, server information, and trap destination configuration, respectively.

```
show snmp communities

show snmp transport

show snmp server

show snmp accesses

show snmp notifies

show snmp trap history
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show srp

Displays the Service Redundancy Protocol (SRP) information.

Product

All products that support Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show srp { audit-statistics [all | instance *number* **] [message-level | session-level] | call-loss statistics | checkpoint statistics [active | standby] [verbose] | info | monitor [all | authentication-probe | bfd | bgp | diameter] | statistics } | [grep** *grep_options* **| more]**

---

audit-statistics [all | instance *number* **] [message-level | session-level]**

Displays statistics of external audit.
all: Displays information for all Session Managers.
instance *number*: Displays information for an instance number of Session Manager.specified as an integer from 1 through 4294967295.
message-level: Displays message-level statistics.
session-level: Displays session-level statistics.

---

call-loss statistics

Displays history of lost calls during switchover.

---

checkpoint statistics [active | standby] [verbose]

Displays check pointing statistics on session redundancy data (session managers, current call recovery records, etc.).
active: Displays information for the active chassis.
standby: Displays information for the standby chassis.
verbose: Displays cumulative information for all session managers in tabular output.

---

info

Displays Service Redundancy Protocol information (context, chassis state, peer, connection state, etc.).

---

monitor [all | authentication-probe | bfd | bgp | diameter]

Displays SRP monitor information.
all: Displays monitor information for all types (authentication-probe, bgp, and diameter).
authentication-probe: Displays authentication probe monitor information.
bfd: Displays BFD monitor information.
bgp: Displays BGP monitor information.
diameter: Displays Diameter monitor information.

---

statistics

Displays SRP statistics (hello messages sent, configuration validation, resource messages, switchovers, etc.).

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

The output of this command may be considered as part of a periodic system auditing program by verifying the Service Redundancy Protocol performance. For more information, refer to the *Interchassis Session Recovery* appendix of the *System Administration Guide* and the *Service Redundancy Protocol Configuration Mode* chapter of this guide.

Example

The following commands display Service Redundancy Protocol information:

```
show srp audit-statistics

show srp call-loss statistics

show srp checkpoint statistics

show srp info

show srp monitor

show srp statistics
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ss7-routing-domain

This command displays the configuration information for the defined Signalling System #7 (SS7) routing domains. Since SS7 routing domains encompass a large number of operational parameters, this command enables you to narrow your displays to specific protocol parameters on a specific link.

Product

SGSN

Privilege

Security Administrator, Administrator, Inspector, Operator

Syntax

show ss7-routing-domain { all | *ss7rd_id* { m3ua | mtp2 | mtp3 | qsaal | routes [adjacent] | sctp asp { all | instance *asp_id* } | sscf } }

show ss7-routing-domain *ss7rd_id* m3ua { statistics { gen | peer-server { all | id *peer-server_id* peer-server-process { all | instance *psp_instance* } } } | status { address-translation-table | destination-point-code { all | *ss7_dpc* } | gen | peer-server *peer-server_id* [peer-server-process instance *psp_id* | verbose] }

show ss7-routing-domain 1 sscf { statistics linkset { all | id *linkset_id* link { all | id *link_id* } } | status linkset { all | id *linkset_id* link { all | id *link_id* [verbose] } } }

ss7-routing-domain { all | *ss7rd_id* }

all: Displays information for all SS7 routing domains.
ss7rd_id: Displays information for the SS7 routing domain ID specified as an integer from 1 through 12.

m3ua

Displays statistics and status information for the SS7 MTP3 User Adaptation Layer (M3UA) in the specified SS7 routing domain.

mtp2

Displays statistics and status information for the SS7 Message Transfer Part-2 (MTP2) in the specified SS7 routing domain.

mtp3

Displays statistics and status information for the SS7 Message Transfer Part-3 (MTP3) in the specified SS7 routing domain.

qsaal

Displays statistics and status information for the Service Specific Connection-Oriented Protocol (SSCOP) sub-layer of the Quasi Signaling Application Adaptation Layer (QSAAL) in the specified SS7 routing domain.

routes [adjacent]

Displays the destination point code (DPC) routing table.

adjacent: If this keyword is used with the **routes** keyword, access is provided to the statistics and status information for configured adjacent point codes.

---

sctp asp { all | instance *asp_id* **}**

Provides access to the status or statistics for the Stream Control Transmission Protocol (SCTP) application server processes (ASP) in the specified SS7 routing domain for all or a specified SCTP ASP instance.

- **all**: Displays the information for all SCTP application server process instances for a specific SS7 routing domain.
- **instance** *asp_id*: Displays the information for an SCTP application server process instance specified as an integer from 1 through 4.

---

sscf

Displays statistics and status information for the Service Specific Coordination Function (SSCF [q.2140]) in the specified SS7 routing domain.

---

peer-server [all | id *peer-server_id* **]**

Filters the information for the specific protocol in the SS7 routing domain for all or a specific peer server ID.

- **all**: Displays the information for all peer servers for a specific protocol.
- **id** *peer-server_id*: Indicates the specific linkset identifier as an integer from 1 through 49.

---

peer-server-process [all | instance *instance_id* **]**

Filters the information for the specific protocol in the SS7 routing domain for all or a specific instance of peer-server process.

- **all**: Displays the information for all peer server process instances for a specific protocol.
- **instance** *instance_id*: Specifies a peer server process instance as an integer from 1 through 4.

---

destination-point-code [all | *dest_point_code***]**

Filters the information for the specific protocol in the SS7 routing domain for all or a specific DPC.

- **all**: Displays the information for all DPCs in the SS7 routing domain.
- *dest_point_code*: Specifies a DPC in the SS7 routing domain.

---

gen

Displays general information for the specific protocol in the specified SS7 routing domain.

---

verbose

Enables the display of maximum information for a protocol.

---

linkset [all | id *linkset_id* **]**

Filters the information for the specific protocol in SS7 routing domain for all or a specific link set.

- **all**: Displays the information for all linkset for a specific protocol.
- **id** *linkset_id*: Specifies a linkset identifier as an integer from 1 through 49.

---

link [all | id *link_id* **]**

Filters the information for a specified protocol in the SS7 routing domain for all or a specific link set.

- **all**: Displays the information for all links for a specific protocol.

- **id** *link_id*: Specifies a linkset identifier as be an integer from 1 through 16.

Usage

Use this command to display the SS7 routing domain and different layer protocol information for SGSN service.

Example

Displays the information/statistics for all SCTP application server processes of peer server ID 17 and peer server process instance 1 in SS7 routing domain 12:

```
show ss7-routing-domain 12 sctp asp all status peer-server id 17 peer-
server-process instance 1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show ssh key

Displays the secure shell (SSH) public key information.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show ssh key [type { v1-rsa | v2-rsa | v2-dsa }] [| { grep *grep_options* **| more }]**

[type { v1-rsa | v2-rsa | v2-dsa }]

Specifies the type of SSH key information to display. If type is not specified, information for all types is displayed.
v1-rsa: SSH v1 RSA host key only
v2-rsa: SSH v2 DSA host key only
v2-dsa: SSH v2 RSA host key only

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Show the secure shell key information for all types to verify installed keys.

Example

The following command shows information for all SSH V1 and SSH V2 keys:

```
show ssh key
```

The following command shows information for only SSH V2 RSA host keys:

```
show ssh key type v2-rsa
```

show ssl cipher-suite

Displays information related to Secure Sockets Layer (SSL) cipher suites since the last restart or **clear** command. A cipher suite contains the cryptographic algorithms supported by the client.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator, Inspector, Operator

Syntax

show ssl cipher-suite [name *name* **] [| { grep** *grep_options* **| more }]**

name *name*

Displays information related to the SSL cipher suite specified as an alphanumeric string of 1 through 127 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information related to SSL cipher suites.

Example

The following command displays information for the SSL cipher suite *ssl_cipher_suite_1*:

```
show ssl cipher-suite name ssl_cipher_suite_1
```

show ssl connection

Displays information pertaining to Secure Sockets Layer (SSL) connections on the Proxy Call Session Control Function (P-CSCF).

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator, Inspector, Operator

Syntax

show ssl connection [list | summary [service-name *name* **]] [name** *name* **] [| { grep** *grep_options* **| more }]**

list

Lists the SSL connections on the P-CSCF.

summary

Displays state and statistical information for the SSL connections on the P-CSCF.

service-name *name*

Lists the SSL connections on the P-CSCF for the specified P-CSCF service, or displays state and statistical information for the SSL connections on the P-CSCF for the specified P-CSCF service.
name must be an alphanumeric string of 1 through 63 characters.

name *name*

Displays state and statistical information for the SSL connection specified as an alphanumeric string of 1 through 127 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command in Exec Mode to display information and statistics pertaining to SSL connections.
If the **summary** keyword is not used, detailed information is displayed.

Example

The following command displays SSL connection information for the P-CSCF service *pcscf_tls_1*:

```
show ssl connection list service-name pcscf_tls_1
```

show ssl map

Displays information related to configured Secure Sockets Layer (SSL) maps/templates since the last restart or **clear** command.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator, Inspector, Operator

Syntax

show ssl map [map-type ssl-subscriber-template] [name *name* **] [| { grep** *grep_options* **| more }]**

map-type ssl-subscriber-template

Displays information related to configured SSL maps/templates for the SSL map/template type ssl-subscriber-template.

name *name*

Displays information related to configured SSL maps/templates for the map/template name specified as n alphanumeric string of 1 through 127 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display information related to configured SSL maps/templates.

Example

The following command displays information related to configured SSL maps/templates for the SSL map/template *ssl_template_1*:

```
show ssl map name ssl_template_1
```

show ssl statistics

Displays statistics for Secure Sockets Layer (SSL) since the last restart or **clear** command.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator, Inspector, Operator

Syntax

show ssl statistics [service-name *name* **] [| { grep** *grep_options* **| more }]**

service-name *name*

Displays SSL statistics for the Proxy Call Session Control Function (P-CSCF) service. specified as an alphanumeric string of 1 through 127 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display SSL statistics.

Example

The following command displays SSL statistics for all P-CSCF services:

```
show ssl statistics
```

show subscribers

Shows information for subscriber sessions defined by the specified keywords. Keywords described under Command Keywords below are base commands that display distinctive types of data. Keywords described under Filter Keywords modify or filter the output of the base commands. Not all filter keywords are available for all command keywords. Each command keyword lists the filter keywords that it accepts.

Product

All

Privilege

Security Administrator, Administrator, Inspector, Operator

Syntax

show subscribers [*command_keyword* **] [** *filter_keywords* **] [| { grep** *grep_options* **| more }]**

command_keyword

The following keywords are base commands that each have a distinct display output. Only one Command Keyword can entered on the command line.

aaa-configuration

Displays Authentication Authorization and Accounting (AAA) configuration information for subscriber sessions defined by the specified filter keywords. The following filter keywords are valid with this command: **active, all, apn, callid, card-num, configured-idle-timeout, connected-time, dhcp-server, dormant**, **fa**, **fa-service, ggsn-service**, ha, ha-service, idle-time, imsi, ip-address, ip-pool, lac, lac-service, lns, lns-service, long-duration-time-left, msid, network-requested, network-type, pcf, pdsn-service, **plmn-type, rx-data**, **session-time-left, sgsn-address**, **sgsn-service, tx-data, username, verbose, grep, more**

access-flows { accounting | dynamic | pre-provisioned | static }

Shows the ip-flows for the subscribers defined by the specified filter keywords.
accounting: displays the accounting type of access flows for a subscriber.
dynamic: displays the dynamic type of access flows for a subscriber.
pre-provisioned: displays the pre-provisioned type of access flows for a WiMAX subscriber.
static: displays the static type of access flows for a subscriber.
The following filter keywords are valid with this command:

active, active-charging-service, all, asngw-service, asnpc-service, asn-peer-address, apn, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, fa, fa-service, flow-type, ggsn-service, gsm-traffic-class, hnbgw-only, ha, ha-ipsec-only, ha-service, idle-time, imsi, ip-address, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-address, l3-tunnel-remote-address, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, msid, msiddn, network-requested, network-type, pcf, pdsn-service, plmn-type, rulebase, rx-data, session-time-left, sgsn-address, sgsn-service, tpo, tx-data, username, verbose, grep, more

activity

Displays subscriber link activity percentage. When no Filter Keywords are specified, the output is a summary of all subscriber activity. When Filter Keywords are specified, the link activity percentage is displayed as graphs in which one is displayed using a high sampling rate, a 10-second interval between samples, and a low sampling rate, a 15-minute interval between samples
The following filter keywords are valid with this command:

```
active, all, asngw-service, asnpc-service, asn-peer-address, apn,
callid, card-num, configured-idle-timeout, connected-time, dhcp-server,
dormant, fa, fa-service, ggsn-service, ha, ha-service, idle-time, imsi,
ip-address, ip-pool, lac, lac-service, lns, lns-service, long-duration-
time-left, msid, network-requested, pcf, pdsn-service, plmn-type, rx-
data, session-time-left, sgsn-address, sgsn-service, tpo, tx-data,
username, grep, more
```

asn-peer-address *ip_address*

Displays information for subscribers on an ASN-GW trusted peer.
ip_address is the IP address of the ASN-GW peer server expressed in IPv4 dotted-decimal notation.
The following filter keywords are valid with this command:

```
all, counters all, asngw-service, full, summary, grep, more
```

asngw-service *service_name*

Displays counters for subscribers accessing the ASN-GW service.
service_name must be an existing service and be from 1 to 63 alphanumeric characters.
The following filter keywords are valid with this command:

```
all, counters all, full, summary, grep, more
```

asnpc-service *service_name*

Displays counters for subscribers accessing the ASN Paging Controller and Location Registry service.
service_name must be an existing Access Service Network Paging Controller (ASN PC) service and be from 1 to 63 alphanumeric characters.
The following filter keywords are valid with this command:

```
all, counters all, full, summary, grep, more
```

bearer-establishment { direct-tunnel | normal | pending }

Selects Bearer Establishment type defined by the specified filter keywords.
direct-tunnel: Select subscribers having direct tunnel established with the Radio Network Controller (RNC).
normal: Select subscribers having bearer established with SGSN.
pending: Select subscribers for whom bearer is not fully established.

configuration

Displays current configuration for all subscribers or a specified subscriber. The following filter keywords are valid with this command:
all, username, grep, more

counters

Shows the counters associated with the subscriber. The following filter keywords are valid with this command:

`active, all, asngw-service, asnpc-service, asn-peer-address, apn, callid, card-num, configured-idle-timeout, connected-time, dhcp-server, dormant, fa, fa-service, ggsn-service, ha, ha-service, idle-time, imsi, ip-address, ip-pool, lac, lac-service, lns, lns-service, long-duration-time-left, msid, network-requested, network-type, pcf, pdsn-service, plmn-type, rx-data, session-time-left, sgsn-address, sgsn-service, tpo, tx-data, username, grep, more`

cscf-only

Displays information for Call Session Control Function (CSCF) subscribers only.
The following filter keywords are valid with this command:

`aaa-configuration, access-flows, active, activity, all, bearer-establishment, callid, card-num, configured-idle-timeout, connected-time, counters, cscf-service, data-rate, dormant, fa, full, gtp-version, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, network-type, policy, rx-data, session-time-left, smgr-instance, subscription, summary, tft, tx-data, username, wf1`

cscf-service *service_name*

Displays information for subscribers accessing the specified CSCF service.
service_name must be an existing service expressed as an alphanumeric string of 1 through 63 characters.
The following filter keywords are valid with this command:

`bearer-establishment, callid, card-num, configured-idle-timeout, connected-time, cscf-service, fa, gtp-version, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, network-type, rx-data, session-time-left, smgr-instance, subscription, tx-data, username`

css-delivery-sequence

Important: This is a restricted keyword. In StarOS 9.0 and later, this keyword is obsoleted.

css-service *csssvc_name*

Important: This is a restricted keyword. In StarOS 9.0 and later releases, this keyword is obsolete.

data-rate [summary | full] [verbose | graph { high | low }] [high | low]

Indicates how to display subscriber throughput data.

Important: This keyword is best used for individual subscriber output.

summary: Combines statistics for the matching subscriber and displays a summary in text form.
full: Displays a separate output for each matching subscriber separately in tabular form.
verbose: Displays cumulative information for all matching subscribers in tabular output.
graph { **high** | **low** }: Display the throughput data as a graph using either a high sampling rate of every 30 seconds or a low sampling rate of every 15 minutes. The graph contains data points over the last 24 hours, if available. The command displays a graph each for the transmit and receive peak, average, and sustained throughput for a total of six graphs.
high: Display the raw data collected for the throughput analysis using a high sampling rate (smaller interval). The data displayed uses a sampling interval of 30 seconds and includes the data collected over the last 24 hours, if available.
low: Display the raw data collected for the throughput analysis using a low sampling rate (larger interval). The data displayed uses a sampling interval of 15 minutes and includes the data collected over the last 24 hours, if available.
The following filter keywords are valid with this command:

```
active, all, asngw-service, asnpc-service, asn-peer-address, apn,
callid, card-num, configured-idle-timeout, connected-time, dhcp-server,
dormant, fa, fa-service, ggsn-service, ha, ha-service, hnbgw-
service,hsgw-only, hsgw-service, idle-time, imsi, ip-address, ip-pool,
lac, lac-service, lma-service, lns, lns-service, long-duration-time-
left, mag-service, mme-address, mme-service, msid, network-requested,
pcf, pdsn-service, plmn-type, rx-data, session-time-left, sgsn-address,
sgsn-service, tpo, tx-data, username, grep, more
```

debug-info { callid *id* **| msid** *id* **| username** *name* **}**

Displays internal call troubleshooting information for subscriber sessions defined by the specified keywords.
callid *id*: Displays subscriber information for the call specified by *id*. The call ID must be specified as an 8-digit hexadecimal number.
msid *id*: Displays information for the mobile user identified by *id*. *id* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘). For example; ‘$’.
username *name*: Displays information for connections for the subscriber identified by *name*. The user must have been previously configured. *name* must be a sequence of characters and/or wildcard characters ('$' and '*') from 1 to 127 characters. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes (‘). For example; ‘$’.

ebi *number*

Displays subscribers based on an EPS bearer identity. *number* specifies the EBI number and must be an integer value from 5 to 15.

enodeb-address *ip_address*

Displays subscribers based on the eNodeB to which they are attached. *ip_address* must be a valid IP address of an existing eNodeB specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

fng-only

Displays Femto Network Gateway (FNG) context information for the session.

fng-service *service_name*

Displays information for subscribers accessing the specified FNG service.
service_name must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

full

Shows all available subscriber information. The following filter keywords are valid with this command:

`active, all, asngw-service, asnpc-service, asn-peer-address, apn, callid, card-num, configured-idle-timeout, connected-time, dhcp-server, dormant, fa, fa-service, ggsn-service, ha, ha-service, idle-time, imsi, ip-address, ip-pool, lac, lac-service, lns, lns-service, long-duration-time-left, msid, network-requested, network-type, pcf, pdsn-service, plmn-type, rx-data, session-time-left, sgsn-address, sgsn-service, tpo, tx-data, username, grep, more`

ggsn-only

Displays only GGSN-specific subscriber context information.

gprs-only

This keyword is specific to the SGSN and only displays 2G SGSN subscriber information.
The following filter keywords are valid with this keyword:

`apn, callid, card-num, connected-time, idle-time, gprs-service, gsm-traffic-class, gtp-version, imsi, msid, msisdn, nri, nsei, sgsn-service, smgr-instance`

gprs-service *srvc_name*

Enter the name of the configured 2G GPRS service to display subscriber information specific to the named GPRS service for the SGSN.
srvc_name must be an alphanumeric string of 1 through 63 characters that identifies a configured GPRS service.
The following filter keywords are valid with this command:

`apn, callid, card-num, connected-time, idle-time, gprs-service, gsm-traffic-class, gtp-version, imsi, msid, msisdn, nri, nsei, sgsn-service, smgr-instance`

gtp-version { 0 | 1 }

Displays the specific GTP version number. Must be followed by one of the supported GTP versions (0 or 1).
The following filter keywords are valid with this command:

`active-charging-service, apn,bearer-establishment, callid, dhcp-server, fa, fa-service, ggsn-service, gprs-service, gsm-traffic-class, msid, msisdn, plmn-type, sgsn-address, sgsn-service, smgr-instance, tx-data, username, grep, more.`

hnbgw-only

Displays HNB-GW subscriber session information.
The following filters/keywords are valid with this command:

```
all, full, summary
```

hnbgw-service *svc_name*: Displays subscriber information based on the HNB-GW service name. *svc_name* must be an existing HNB-GW service expressed as an alphanumeric string of 1 through 63 characters.

---

hsgw-only

Displays HSGW subscriber session information.
The following filters/keywords are valid with this command:

```
all, full, summary
```

hsgw-service *svc_name*: Displays subscriber information based on the HSGW service name. *svc_name* must be an existing HSGW service expressed as an alphanumeric string of 1 through 63 characters.

---

hsgw-service *svc_name*

Displays subscriber information based on the HSGW service name. *svc_name* must be an existing HSGW service expressed as an alphanumeric string of 1 through 63 characters.

---

imsi *imsi*

Displays information specific to one subscriber or group of subscribers. Enter 1 to 15 digits to identify a specific subscriber's IMSI (International Mobile Subscriber Identity).
The following filter keywords are valid with this command:

```
apn, callid, card-num, connected-time, idle-time, gprs-service, gsm-traffic-class, gtp-
version, imsi, msid, msisdn, nri, nsei, sgsn-service, smgr-instance
```

---

ip-alloc-method {aaa-assigned | dhcp [relay-agent | proxy-client] | dynamic-pool | l2tp-lns-assigned | mip-ha-assigned | ms-provided-static | not-ms-provided-static | static pool }

Displays the specific IP Allocation Method. Must be followed by one of the IP Allocation Methods:
aaa-assigned: Selects subscribers whose IP addresses were assigned by AAA.
dhcp: Selects subscribers whose IP addresses were assigned by DHCP.

- **relay-agent**: Selects subscribers whose IP addresses were assigned by the DHCP Relay Agent
- **proxy-client**: Selects subscribers whose IP addresses were assigned by the DHCP Proxy Client

dynamic-pool: Selects subscribers whose IP addresses were assigned from a dynamic IP address pool.
l2tp-lns-assigned: Selects subscribers whose IP addresses were assigned by the Layer 2 Tunneling Protocol (LT2P) Network Server.
mip-ha-assigned: Selects subscribers whose IP addresses were assigned by the Mobile IP Home Agent.
ms-provided-static: Selects subscribers whose IP addresses were provided by the Mobile Station.
not-ms-provided-static: Selects subscribers whose IP addresses were not provided by the Mobile Station.
static-pool: Selects subscribers whose IP addresses were assigned from a static IP address pool.

---

ipsg-only

Displays IPSG subscriber session information.

---

lma-service *svc_name*

Displays subscriber information based on the Local Mobility Anchor (LMA) service name. *svc_name* must be an existing LMA service expressed as an alphanumeric string of 1 through 63 characters.

mag-only

Displays MAG subscriber session information.
The following filters/keywords are valid with this command:

```
all, full, summary
```

mag-service *svc_name*: Displays subscriber information based on the Mobile Access Gateway (MAG) service name. *svc_name* must be an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

mag-service *svc_name*

Displays subscriber information based on the MAG service name. *svc_name* must be an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

mme-address

Displays subscriber information based on the MME IP address. *ip_address* must be an existing MME IP address and be entered in IPv4 dotted-decimal notation.

mme-only

Displays MME subscriber session information.
The following filter keywords are valid with this command:

```
all, full, summary
```

mme-service *svc_name*: Displays subscriber information based on the MME service name. *svc_name* must be an existing MME service expressed as an alphanumeric string of 1 through 63 characters.
mme-address *ip_address*: Displays subscriber information based on the MMM IP address. *ip_address* must be an existing MME IP address entered in IPv4 dotted decimal notation.

mseg-only

Important: This keyword is not supported in this release. For more information please contact your Cisco account representative.

Displays MSEG-specific subscriber information.
The following filter keywords are valid with this option:

```
all, apn, callid, card-num, full, fw-and-nat, gsm-traffic-class, imsi,
ip-alloc-method, mseg-service, network-type, rulebase, smgr-instance,
subscription, summary, tft
```

mseg-service *mseg_service_name*

Important: This keyword is not supported in this release. For more information please contact your Cisco account representative.

Displays MSEG service specific subscriber information.
mseg_service_name must be the name of an existing MSEG service, expressed as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this option:

```
active-charging-service, apn, bandwidth-policy, bearer-establishment,
bng-service, callid, card-num, cbb-policy, configured-idle-timeout,
connected-time, dhcp-server, ebi, enodeb-address, fa, firewall, fw-and-
nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, ha,
idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool,
ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr,
long-duration-time-left, mipv6ha-service, mseg-service, msid, msisdn,
nat, network-requested, network-type, plmn-type, profile-id, qci,
rulebase, rx-data, s1u-state, s5-proto, session-time-left, sgsn-address,
sgsn-service, smgr-instance, tpo, tx-data, username
```

msid *msid*

For this SGSN-specific keyword, enter the MSID (Mobile Station IDentifier) to display information specific to one subscriber's equipment by entering the MSID.
The following filter keywords are valid with this command:

```
apn, callid, card-num, connected-time, idle-time, gprs-service, gsm-traffic-class, gtp-
version, imsi, msid, msisdn, nri, nsei, sgsn-service, smgr-instance
```

msisdn *msisdn*

For this SGSN-specific keyword, enter the MSISDN (Mobile Station ISDN number - unique SIM phone number) to display information specific to one subscriber's equipment by entering the MSISDN.
The following filter keywords are valid with this command:

```
apn, callid, card-num, connected-time, idle-time, gprs-service, gsm-traffic-class, gtp-
version, imsi, msid, msisdn, nri, nsei, sgsn-service, smgr-instance
```

pdg-only

Displays a summary of PDG subscriber statistics.

pdg-service *name*

Displays statistics for users associated with a specific PDG service name.

pdif-only

Displays a summary of Packet Data Interworking Function (PDIF) subscriber statistics.

pdif-service *name*

Displays connection statistics for users associated with a specific PDIF service name.

pgw-only

Displays PDN-Gateway (P-GW) subscriber session information.
The following filters/keywords are valid with this command:

```
all, full, summary
```

pgw-service *svc_name*: Displays subscriber information based on the P-GW service name. *svc_name* must be an existing P-GW service expressed as an alphanumeric string of 1 through 63 characters.

sgw-address *ip_address*: Displays subscriber information based on the S-GW IP address. *ip_address* must be an existing S-GW IP address in IPv4 dotted-decimal notation.

---

qci *number*

Displays subscriber session information based on the QoS Class Identifier (QCI) value assigned to the subscriber. *number* must be an integer value from 0 to 9.

---

s1u-state { active | idle | idle-active }

Displays session information based on the subscriber's S1-U state. The S1-U interface is the interface from the eNodeB to the S-GW.
active: Displays session information for subscribers with an S1-U state set to active.
idle: Displays session information for subscribers with an S1-U state set to idle.
idle-active: Displays session information for subscribers with an S1-U state set to idle-active.

---

s5-proto { gtp | pmip }

Displays subscriber session information based on the S5 interface protocol used. Choose either GPRS Tunneling Protocol (GTP) or Proxy Mobile IPv6 (PMIP).

---

sgsn-only

This SGSN-only keyword displays only 3G SGSN-specific subscriber context information.
The following filter keywords are valid with this command:

```
apn, callid, card-num, connected-time, idle-time, gprs-service, gsm-traffic-class, gtp-
version, imsi, msid, msisdn, nri, nsei, sgsn-service, smgr-instance
```

---

sgsn-service *service_name*

For this SGSN-only keyword, enter the name of the configured 3G SGSN service to display subscriber information specific to the named SGSN service.
The following filter keywords are valid with this command:

```
apn, callid, card-num, connected-time, idle-time, gprs-service, gsm-traffic-class, gtp-
version, imsi, msid, msisdn, nri, nsei, sgsn-service, smgr-instance
```

---

sgw-only

Displays S-GW subscriber session information.
The following filters/keywords are valid with this command:

```
all, full, summary
```

sgw-service *svc_name*: Displays subscriber information based on en existing S-GW service specified as an alphanumeric string of 1 through 63 characters.
pgw-address *ip_address*: Displays subscriber information based on an existing P-GW specified by its IP address in IPv4 dotted-decimal notation.

---

sgw-service *svc_name*

Displays subscriber information based on an existing S-GW service specified as an alphanumeric string of 1 through 63 characters.

subscription { aor *address* **| callid** *id* **| full }**

Displays subscription information for defined subscribers, based on defined parameters.
aor *address*: Clears session(s) by Address of Record.
callid *id*: Specifies a Call Identification Number.
full: Displays all available information.

summary

Displays only a summary of the subscriber information. The following filter keywords are valid with this command:

`active, active-charging-service, activity, all, asngw-service, asnpc-service, asn-peer-address, apn, bandwidth-policy, bearer-establishment, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, dhcp-server, dormant, enodeb-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, ha, ha-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, lac, lac-service, lns, lns-service, long-duration-time-left, mseg-service, msid, msisdn, nat, network-requested pcf, pdsn-service,plmn-type, profile-id, qci, rulebase, rx-data, session-time-left, sgsn-address, tpo, tx-data, username, grep, more`

tft

Displays the current Traffic Flow Template (TFT) associated with the subscriber session.

tx-data

Bytes transmitted by the subscriber.

wf1

Displays subscriber information in wide format number 1. Wide format number 1 includes the following information for each listed subscriber session:

- Access Type
- Access Technology
- Call State
- Link Status
- Network Type
- Call ID
- MSID
- Username
- IP Address
- Time-Idle
- Access Peer Address
- Service Address
- Network Peer Address
- Connect Time

filter_keywords

The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all Command Keywords. Multiple Filter Keywords can be entered on a command line. When multiple Filter Keywords are specified, the output conforms to all of the Filter Keywords specifications.
For example; if you enter the following command:
show subscribers counters ip-pool pool1 card-num 1
Counters for all subscriber sessions that were assigned an IP address from the IP pool named pool1 and also are being processed by the processing card in slot 1 is displayed. Information for all other subscribers is not displayed.

active

Only display information for those subscribers who currently have active sessions.

active-charging-service *acs_service*

Displays information for subscribers being processed by the active charging service specified as an alphanumeric string of 1 through 15 characters.

all

If no keywords are specified before **all**, information for all subscribers is displayed. If keywords are specified before **all**, all information is displayed with no further options being allowed.

apn *name*

Displays subscribers currently facilitated by the access point name (APN) configured on the SGSN or GGSN.

asngw-only

Displays counters for subscribers accessing the ASN-GW service only.

asnpc-only

Displays counters for subscribers accessing the ASN Paging Controller and Location Registry service only.

hnbgw-only

Displays counters for subscribers accessing the HNB-GW service only.

callid *id*

Displays subscriber information for the call ID specified as an 8-byte hexadecimal number.

card-num *card_num*

The slot number of the processing card by which the subscriber session is processed. The slot number is an integer from 1 through 74 or 10 through 16.

ccoa-only

Displays the subscribers that registered a MIP with CoA directly with the HA.
This option is only valid when a MIPHA session license is enabled.

configured-idle-timeout [< | > | greater-than | less-than] *value*

Shows the idle timeout that is configured for the specified subscriber. A value of 0 (zero) indicates that the subscribers idle timeout is disabled.
<: Filters output so that only information less than the specified value is displayed.
>: Filters output so that only information greater than the specified value is displayed.
greater-than: Filters output so that only information greater than the specified value is displayed.
less-than: Filters output so that only information less than the specified value is displayed.
value: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

connected-time [< | > | greater-than | less-than] *value*

Shows how long the subscriber has been connected. **<**: Filters output so that only information less than the specified value is displayed.
<: Filters output so that only information less than the specified value is displayed.
>: Filters output so that only information greater than the specified value is displayed.
greater-than: Filters output so that only information greater than the specified value is displayed.
less-than: Filters output so that only information less than the specified value is displayed.
value: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

cscf-only

Displays information for Call Session Control Function (CSCF) subscribers only.

cscf-service *service_name*

Displays information for subscribers accessing an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.

dhcp-server *address*

Displays subscribers currently accessing the system that have been provided an IP address by the DHCP server specified by its address. GGSN only.

dormant

Shows information for subscriber sessions that are dormant (not transmitting or receiving data).

enodeb-address *IPv4_ddress*

Displays information for Evolved Packet System (EPS) subscribers connected to the eNodeB specified by IP address in IPv4 dotted-decimal notation.

fa *address*

Displays information for subscribers connected to the foreign agent specified by its IP address in IPv4 dotted-decimal notation.

fa-only

Only display FA-specific context information.

fa-service *name*

Displays information for subscribers connected to the named foreign agent (FA) service.

firewall { not-required | required }

Displays information for the specified subscribers:
not-required: Subscribers for whom firewall processing is not required.
required: Subscribers for whom firewall processing is required.

firewall-policy *fw_policy_name*

This keyword is obsolete.

fw-and-nat policy *fw_nat_policy*

Important: This option is customer-specific and is only available in StarOS 8.1.

Displays information for subscribers using an existing Firewall-and-NAT policy specified as an alphanumeric string of 1 through 15 characters.

ggsn-address *ip_address*

Displays information for subscribers connected to an existing GGSN specified by its IP address in IPv4 doted-decimal notation. SGSN only

ggsn-preservation-mode

Displays information for subscribers connected to the GGSN service with preservation mode enabled. GGSN only.

ggsn-service *name*

Displays information for subscribers connected to the named GGSN service. This keyword is for GGSN only.

gprs-only

Displays only 2G SGSN subscribers content. SGSN only.

gprs-service *srvc_name*

Displays subscriber information for the named 2G GPRS service. SGSN only.

gsm-traffic-class { background | conversational | interactive | streaming }

Displays information for subscriber traffic that matches the specified 3GPP traffic class.

- **background**: 3GPP QoS background class.
- **conversational**: 3GPP QoS conversational class.
- **interactive**: 3GPP QoS interactive class. Must be followed by a traffic priority.
- **streaming**: 3GPP QoS streaming class.

ha *address*

Displays information for subscribers connected to the home agent specified by its IP address in IPv4 dotted-decimal notation.

ha-ipsec-only

Only displays information for subscriber sessions that are using IP-Security (IPSec).

ha-only

Only displays HA-specific context information.

ha-service *name*

Displays information for subscribers connected to the named home agent service.

idle-time [< | > | greater-than | less-than] *value*

Displays how long the subscriber session has been idle or display subscriber sessions that meet the idle time criteria specified.
<: Filters output so that only information less than the specified value is displayed.
>: Filters output so that only information greater than the specified value is displayed.
greater-than: Filters output so that only information greater than the specified value is displayed.
less-than: Filters output so that only information less than the specified value is displayed.
value: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

ims-auth-service *service_name*

Displays information for subscribers for an existing IMS Authorization Service name.

imsi *id*

Displays the subscriber with the specified ID. The IMSI (International Mobile Subscriber Identity) ID is a 15-character string which identifies the subscriber's home country and carrier. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘). For example; ‘$’.

ip-address [< | > | greater-than | less-than] *address*

Displays information for subscribers connected to the specified *address*.
<: Filters output so that only information for subscribers with an IP address lower than the specified address is displayed.
>: Filters output so that only information for subscribers with an IP address higher than the specified address is displayed.
greater-than: Filters output so that only information for subscribers with an IP address higher than the specified address is displayed.
less-than: Filters output so that only information for subscribers with an IP address lower than the specified address is displayed.
address: The address must be specified using IPv4 dotted-decimal notation. Used in conjunction with <, >, greater-than, less-than. If the IP address is specified without a qualifier, only subscribers with the specified IP address have their information displayed.

ip-pool *name*

Displays information for subscribers assigned addresses from an existing IP address pool or IP pool group. *name* will be an IP address in IPv4 dotted-decimal or IPv6 colon-separated notation based on the call line setup for the specified pool.

ipv4

Displays information for subscribers with an IPv4 Firewall enabled/disabled.

ipv6

Displays information for subscribers with an IPv6 Firewall enabled/disabled.

ipv6-address *address*

Displays information for subscribers connected to the specified IPv6 address.

ipv6-prefix *prefix*

Displays information for subscribers connected to the specified IPv6 address prefix.

lac *address*

Displays information for calls to the peer L2TP Access Concentrator (LAC) specified by its IP address.

lac-only

Displays LAC specific information only.

lac-service *name* **[local-tunnel-id id | remote-tunnel-id** *id* **]**

Displays information for calls associated with the LAC service specified as an alphanumeric string of 1 through 63 characters.
local-tunnel-id *id*: Specifies a local tunnel from which to clear calls as an integer from 1 through 65535.
remote-tunnel-id *id*: Specifies a remote tunnel from which to clear calls as an integer from 1 through 65535.

l3-tunnel-local-addr *ip_address*

A layer 3 tunneling interface specified by its IP address in IPv4 dotted-decimal notation.

l3-tunnel-remote-addr *ip_address*

A layer 3 tunneling peer specified by its IP address in IPv4 dotted-decimal notation.

lns *address*

Displays information for calls to the peer L2TP Network Server (LNS) specified by its IP address.

lns-only

Displays LNS specific information only.

lns-service *name* **[local-tunnel-id** *id* **| remote-tunnel-id** *id* **]**

Displays information for calls associated with the LNS service specified as an alphanumeric string of 1 through 63 characters.

local-tunnel-id *id*: Indicates a specific local tunnel from which to clear calls. *id* must be an integer from 1 through 65535.
remote-tunnel-id *id* : Indicates a specific remote tunnel from which to clear calls. *id* must be an integer from 1 through 65535.

---

long-duration-time-left [< | > | greater-than | less-than] *value*

Shows how much time is left for the maximum duration of a specified subscriber session.
<: Filters output so that only information less than the specified value is displayed.
>: Filters output so that only information greater than the specified value is displayed.
greater-than: Filters output so that only information greater than the specified value is displayed.
less-than: Filters output so that only information less than the specified value is displayed.
value: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

---

mip-udp-tunnel-only

Displays the subscribers that negotiated MIP-UDP tunneling with the HA.
This option is only valid when MIP NAT Traversal license is enabled.

---

mipv6ha-only

Displays MIPV6HA-specific context information for the session.

---

mipv6ha-service *service_name*

Displays specific configured MIPV6 Home Agent service. *service_name* must have been previously defined.

---

msid *id*

Displays information for the mobile user identified by *id*. *id* must be from 7 to 16 hexadecimal digits specified as an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘). For example: ‘$’.
In case of **enforce imsi-min equivalence** is enabled on the chassis and MIN or IMSI numbers supplied, this filter will show subscribers with a corresponding MSID (MIN or IMSI) whose lower 10 digits matches to lower 10 digits of the supplied MSID.
show subscribers msid *ABCD0123456789* or
show subscribers msid *0123456789*
will show any subscriber with a MSID that match the lower 10 digits of MSID supplied, for example, 0123456789.

---

msisdn *msisdn*

Displays information for the mobile user identified by the Mobile Subscriber ISDN Number (MSISDN). *msisdn* must be 7 to 16 digits; specified as an IMSI, MIN, or RMI.

---

nat { not-required | required [nat-ip *nat_ip_address* **| nat-realm** *nat_realm* **] } [ipv4 | ipv6]**

Displays information for the specified subscribers.
not-required: Subscribers for whom Network Address Translation (NAT) processing is not required.
required: Subscribers for whom NAT processing is required.

Important: The **nat-ip** keyword is only available in StarOS 8.3 and later releases.

nat-ip *nat_ip_address*: Subscribers for whom NAT processing is enabled and are using the specified NAT IP address. *nat_ip_address* specifies the NAT IP address and must be in IPv4 dotted-decimal notation.
nat-realm *nat_realm*: Subscribers for whom NAT processing is enabled and are using the specified NAT realm. *nat_realm* specifies the NAT realm name and must be a string from 1 through 63 characters.
ipv4: Subscribers for whom NAT44 processing is required.
ipv6: Subscribers for whom NAT64 processing is required.

network-requested

Display information for currently active subscribers whose sessions were initiated by the GGSN network requested create PDP context procedure.

network-type { gre | ipip | ipsec | ipv4 | ipv6 | l2tp | mobile-ip | proxy-mobile-ip }

Displays network type information for the subscriber session. The following network types can be selected:

- **gre**: Generic Routing Encapsulation (GRE) per RFC 2784
- **ipip**: IP-in-IP encapsulation per RFC 2003
- **ipsec**: IPSec
- **ipv4**: Internet Protocol version 4 (IPv4)
- **ipv6**: Internet Protocol version 6 (IPv6)
- **l2tp**: Layer 2 Tunneling Protocol (L2TP) encryption per RFC 2661
- **mobile-ip**: Mobile IP
- **proxy-mobile-ip**: Proxy Mobile IPv6

nri *nri_value*

This SGSN-specific filter uses the configured network resource identifier (NRI) to identify a specific SGSN in a pool to fine-tuned the subscriber information to be displayed.
nri_value: enter an integer from 0 through 63
This filter can be used in combination with further refining filters.

partial qos { negotiated | requested }

This filter is specific to the SGSN.
Is limits the display of information to requested or negotiated QoS information for the subscriber.
This filter can be used in combination with further defining filters: active, active-charging-service, all, apn, callid, card-num, configured-idle-timeout, connected-time, ggsn-address, gprs-service, gsm-traffic-class, idle-time, imsi, msid, msisdn, negotiated, plmn-type, requested, rx-data, session-time-left, tx-data

pcf [< | > | less-than | greater-than] *ipv4_address* **[[< | > | less-than | greater-than]** *ipv4_address* **]**

Displays information for subscribers connected via the packet control function with a specific or range of IP addresses. The address must be specified using IPv4 dotted-decimal notation.

- **<**: Filters output so that only information less than the specified IPv4 address value is displayed.
- **>**: Filters output so that only information greater than the specified IPv4 address value is displayed.

- **less-than**: Filters output so that only information less than the specified IPv4 address value is displayed.
- **greater-than**: Filters output so that only information greater than the specified IPv4 address value is displayed.

Note: It is possible to define a limited range of IP addresses by using the less-than and greater-than options to define minimum and maximum values.

---

pdsn-only

Show PDSN specific information only.

---

pdsn-service *name*

Displays information for subscribers connected to the packet data service *name*. The packet data service must have been previously configured.

---

plmn-type

Displays subscriber type (HOME, VISITING, or ROAMING).
This keyword is for the GGSN or the SGSN only.

---

policy

Displays the current policies associated with the subscriber session.

---

rnc id *rnc_id* **mcc** *mcc_num* **mnc** *mnc_num*

Displays information for subscribers connected to the SGSN via a specific RNC (radio network controller) identified by the RNC ID, the MCC (mobile country code), and the MNC (mobile network code). SGSN only

---

rx-data [< | > | greater-than | less-than] *value*

The number of bytes received by the specified subscriber.
<: Filters output so that only information less than the specified value is displayed.
>: Filters output so that only information greater than the specified value is displayed.
greater-than: Filters output so that only information greater than the specified value is displayed.
less-than: Filters output so that only information less than the specified value is displayed.
value: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 18446744073709551615.

---

session-time-left [< | > | greather-than | less] *value*

How much session time is left for the specified subscriber.
<: Filters output so that only information less than the specified value is displayed.
>: Filters output so that only information greater than the specified value is displayed.
greater-than: Filters output so that only information greater than the specified value is displayed.
less-than: Filters output so that only information less than the specified value is displayed.
value: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

---

smgr-instance *number*

Specific sessmgr instance. *number* must be in the range of 1 to 4294967295.

sgsn-address *address*

Shows information for subscribers whose PDP contexts are currently being facilitated by the SGSN specified by address. This command is for GGSN only.

sgsn-service *srvc_name*

Shows subscriber information for a specified 3G SGSN service.
srvc_name must be an alphanumeric string of 1 through 63 characters that identifies a configured SGSN service.
This command is for SGSN only.

tpo { not-required | required }

Displays information for specified subscribers.

- **not-required**: Subscribers for whom Traffic Performance Optimizer (TPO) processing is not enabled.
- **required**: Subscribers for whom TPO processing is enabled.

tx-data [< | > | greater-than | less-than] *value*

The number of bytes transmitted by the specified subscriber.
<: Filters output so that only information less than the specified value is displayed.
>: Filters output so that only information greater than the specified value is displayed.
greater-than: Filters output so that only information greater than the specified value is displayed.
less-than: Filters output so that only information less than the specified value is displayed.
value: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 18446744073709551615.

username *name*

Displays information for connections for the subscriber identified by *name*. The user must have been previously configured. *name* must be a sequence of characters and/or wildcard characters ('$' and '*') from 1 to 127 characters. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘). For example; ‘$’.

verbose

Display detailed information.

wide-format

Display detailed information in a wider screen format.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view information about subscriber sessions.
The output of this command may be considered for part of a periodic system auditing program by verifying active and dormant subscribers.
The Command Keywords may be used standalone to display detailed information or you may use one or more of the various Filter Keywords to reduce the amount of information displayed.

Caution: Executing this command may negatively impact performance if multiple instances are executed while the system is under heavy load and simultaneously facilitating multiple CLI sessions.

Example

The following command displays information for all subscriber sessions:

```
show subscribers all
```

The following command displays information for all ggsn-only subscriber sessions:

```
show subscribers ggsn-only all
```

The following command displays information for all subscriber sessions in wide format 1:

```
show subscribers wf1 all
```

```
show subscribers aaa-configuration
```

```
show subscribers counters username isp1user1
```

The following command displays information for subscriber in GGSN service:

```
show subscribers ggsn-only allshow subscribers ggsn-only full
```

The following command displays information for all subscriber with SGSN session having partial QoS requests:

```
show subscribers sgsn-only partial qos requested
```

The following command displays information for all subscriber with MME session connected to MME service having IP address as *10.1.1.1*:

```
show subscribers mme-only mme-address 10.1.1.1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show super-charger

Lists subscribers with valid super-charger configuration. When super-charger is enabled for a subscriber, the SGSN handles 2G or 3G connections controlled by an operator policy and changes hand-off and location update procedures to reduce signaling traffic management (3GPP, TS.23.116).

Product

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show super-charger { imsi imsi | all }
```

imsi

Defines a specific subscriber's international mobile subscriber identity (IMSI) number.
imsi is a string of up to 15 digits that includes the MCC (mobile country code), the MNC (mobile network code) and the MSIN (mobile station identification number),

all

Instructs the SGSN to display super charger subscription information for all subscribers.

Usage

Use this command to determine if a single subscriber, identified by the IMSI, has a super charger configuration. Also, this command can display the list of all subscribers with a super charger configuration. If a subscriber has super charger as part of the configuration, subscriber data is backed up (using the IMSI Manager) after the subscriber detaches and the purge timer expires.

Example

The following command displays the super charger configuration information for the subscriber identified by the IMSI 90121882144672.

```
show super-charger imsi 90121882144672
```

show support details

Displays a comprehensive list of system information that is useful for troubleshooting purposes. In most cases, the output of this command is requested by the Technical Assistance Center (TAC).

Product

All

Privilege

All

Syntax

show support details [to file *url* **[compress]]**

to file *url*

Specifies the location where a tar file with the support detail information should be created. *url* may refer to a local or a remote file and must be entered using the following format:
[file:] { /flash | /pcmcia1 | /hd } [/*directory* **] /***file_name* **[compress]**
tftp:// { *host* **[** *:port#* **] } [/***directory* **] /***file_name*
[ftp: | sftp:] // [*username***[** *:password* **] @] {** *host* **} [** *:port#* **] [/***directory* **] /***file_name*

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.
If the filename is not specified with a .tar extension, it is automatically appended to the filename when the file is created and a message is generated.
The content of the tar file is:

- **support_summary** - An ASCII text file that contains the support detail information.
- **information.minicores.tar** - A tar file that contains any minicore files found on the system. Minicore files contain memory core dumps that are captured during some events. These core dumps provide specific memory locations and other information about the event. This information is useful to the technical support team in identifying where and when an event occurred along with its probably cause.

compress

Generates a compressed .tar.gz file for the output of the command.

Usage

Use this command to obtain extensive system information for use in troubleshooting. This command does the work of over 30 separate commands, which saves time and ensures that all of the information needed is collected and displayed in the same order every time.

In addition to the information provided, the show support details command includes information that is not otherwise accessible to users but that is helpful in the swift resolution of issues.

Example

The following command displays the system information on your console.

```
show support details
```

The following command displays the information on your console and also writes it to the local device (pcmcia1 in this case) and includes the mini core dumps, using the filename *r-p_problem.tar*:

```
show support details to file /pcmcia1/r-p_problem.tar
```

The following command displays the information on your console and also writes it to an FTP server (named host), placing the file in the **dir** directory and includes the mini core dumps, using the filename *re_problem.tar*:

```
show support details to file ftp://host/dir/re_problem.tar
```

show system uptime

Displays the amount of time the system has been operational since its last down time (maintenance or otherwise).

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show system uptime [| { grep *grep_options* **| more }]**

uptime

Displays system up time in days (D), hours (H) and minutes (M).

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Display the system up time to check for the possibility of anomalous behavior related to shorter or longer up times.

Example

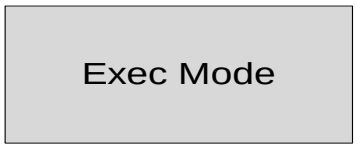
The following command displays basic system basic information and up time.

```
show system uptime
```

Chapter 119
Exec Mode Show Commands (T-Z)

This chapter includes the commands **`show tacacs`** through **`show version`**.

The Exec Mode is the initial entry point into the command line interface system. Exec mode **show** commands are useful in troubleshooting and basic system monitoring.



show tacacs

Displays information about all active Terminal Access Controller Access-Control System Plus (TACACS+) sessions.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax `show tacacs`

This command provides the following TACACS+ session information:

- individual active session number with the following additional session-specific information:
  - login username
  - login tty
  - time of login
  - login server priority
  - current session state
  - current privilege level
  - remote client application (if applicable)
  - remote client ip address (if applicable)
  - last server reply status
- total number of TACACS+ sessions

Usage

Use this command to view detailed session information for all active TACACS+ sessions.

Important: This command is available on version 11.0 and later systems.

Example

```
show tacacs
```

show task

Displays information about system tasks.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show task { info | memory | resources | table } [card *card_num* **] [facility** *facility* **{ all | instance id }] [process** *process_name* **all] [max] [| { grep** *grep_options* **| more }]**

{ info | memory | resources | table }

Specifies the type of information to be displayed and scope of tasks to include in output.
info: Displays detailed task information.
memory: Displays detailed task memory use information.
resources: Displays resource allocation and usage information for all tasks.
table: Displays identification information in tabular format for all tasks.

---

card *card_num*

Default: all powered on cards.
Specifies a single card for which task information is to be displayed where *card_num* must be from 1 to 48.

---

facility *facility* **{ all | instance id }**

Default: all facilities.
Specifies the list of facilities for which task information may be displayed. A specific instance of the facility may be displayed as specified by ID or all instances may be displayed. The value of *id* must be an integer from 0 through 100000. *facility* must be one of:

- **a11mgr**: A11 Interface Manager facility
- **aaamgr**: AAA Manager Facility
- **aaaproxy**: AAA Proxy manager Facility
- **acsctrl**: Active Charging Service (ACS) Controller Facility
- **acsmgr**: Active Charging Service (ACS) Manager Facility
- **asngwmgr**: ASN Gateway Manager
- **asnpcrmg**r: ASN Paging/Location-Registry (ASN-PC) Manager
- **bgp**: Border Gateway Protocol (BGP) Facility
- **bulkstat**: Bulk Statistics Manager Facility
- **cdrmod**: Charging Detail Record Module
- **cli**: Command Line Interface Facility
- **cscfmgr**: SIP CSCF Manager
- **cspctrl**: Card Slot Port controller Facility

- **cssctrl**: Content Service Steering Controller
- **dcardctrl**: IPSEC Daughter-card Controller Logging Facility
- **dcardmgr**: IPSEC Daughter-card Manager Logging Facility
- **dhmgr**: Distributed Host Manager
- **drvctrl**: Driver Controller Facility
- **egtpegmgr**: EGTP Egress Demux Manager
- **egtpinmgr**: EGTP Ingress Demux Manager
- **evlogd**: Event Log Daemon Facility
- **famgr**: Foreign Agent Manager Facility
- **gtpcmr**: GTP-C Protocol Logging facility (GGSN product only)
- **h248prt**: H.248 Protocol Task
- **hamgr**: Home Agent Manager Facility
- **hatcpu**: High Availability Task CPU Facility
- **hatsystem**: High Availability Task Facility
- **ipsecctrl**: IP Security Controller Facility
- **ipsecmgr**: IP Security Manager Facility
- **ipsgmgr**: IP Services Gateway Facility
- **l2tpdemux**: L2TP Demultiplexor (LNS) Facility
- **l2tpmgr**: L2TP Manager Facility
- **magmgr**: Mobile Access Gateway Manager
- **megadiammgr**: MegaDiameter Manager
- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager logging facility
- **mmgr**: SGSN/SS7 Master Manager
- **mptest**: Migration Performance Test on Packet Accelerator Card
- **netwstrg**: Network Storage Manager
- **npuctrl**: Network Processor Unit control Facility
- **npumgr**: Network Processor Unit Manager Facility
- **nputst**: Network Processor Unit Tester
- **nsctrl**: Charging Service Controller
- **nsmgr**: Charging Service Process Manager
- **orbns**: Object Request Broker Notification Server Facility
- **orbs**: Object Request Broker System Facility
- **ospf**: Open Shortest Path First Facility
- **rct**: Recovery Control Task Facility
- **rdt**: Redirect Task Facility
- **rip**: Routing Information Protocol Facility

- **rmctrl**: Resource Manager Controller Facility
- **rmmgr**: Resource Manager Facility
- **sct**: Shared Configuration Task Facility
- **sessctrl**: Session Controller Facility
- **sessmgr**: Session Manager Facility
- **sft**: Switch Fabric Monitoring Task
- **sipcdprt**: Sip Call Distributor Task
- **sitmain**: System Initialization Task Main Facility
- **sitparent**: Card based system initialization facility that applies to Packet Accelerator Cards and Switch Processor Cards

Important: **sitparent** replaces the facilities **sitpac, sitspc** and **sittac**.

- **snmp**: SNMP Protocol Facility
- **srdb**: Static Rating Database
- **threshold**: Threshold Server Facility
- **vpnctrl**: Virtual Private Network Controller Facility
- **vpnmgr**: VPN Manager Facility
- **zebos**: ZEBOS™ OSPF Message Facility

`all`: Displays information for all instances of the specified facility.
`instance` *`id`*: Displays information for the facility instance specified as an integer from 0 through 10000000.

`process` *`process_name`* **`all`**

Display information for all instances of the specified process. must be one of the following process names:

- **ftpd**: File Transfer Protocol Daemon
- **inetd**: Internet Super-server Daemon
- **nsproc**: NetSpira Packet Processor
- **ntpd**: Network Time Protocol Daemon
- **orbnsd**: Object Request Broker Notification Server
- **ping**: Ping
- **pvmd-wrapper**: NetSpira Messenger Daemon
- **pvmgs**: NetSpira Messenger Daemon
- **rlogin**: Remote Login
- **sftp-server**: Secure File Transfer Protocol Server
- **sitreap**: System Initialization Task Cleanup Process
- **sn_resolve**: DNS Resolver Process
- **ssh**: Secure Shell
- **sshd**: Secure Shell Daemon

- **telnet**: Telnet
- **telnetd**: Telnet daemon
- **tftpd**: Trivial File Transfer Protocol Daemon
- **traceroute**: Traceroute

max

Default: current usage levels are displayed.
Displays the maximum usage levels for tasks as opposed to the current usage levels.
The keyword **max** is valid only in conjunction with the **resources** keyword.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Display task information as part of system troubleshooting unexpected behavior.

Important: This command is not supported on all platforms.

Example

The following commands provide some examples of the combinations of options that may be used to display task information.

```
show task info facility hatspc all

show task info facility hatspc instance 456

show task resources facility zebos all

show task table facility ospf

show task table card 8 facility cli all

show task resources facility rip all max
```

show tcap statistics

This command displays the collected traffic statistics that have passed through the SS7 Transaction Capabilities Application Part (TCAP) layer.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

show tcap statistics [camel-service [all | name *camel_srvc* **] | map-service [all | name** *map_srvc* **]] [| { grep** *grep_options* **| more }]**

camel-service [all | name *camel_srvc* **]**

Displays TCAP statistics for either all Customized Applications for Mobile networks Enhanced Logic (CAMEL) services or only for the named CAMEL service.

map-service [all | name *mapl_srvc* **]**

Displays TCAP statistics for either all Mobile Application Part (MAP) services or only for the named MAP service.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display the collected TCAP statistics for MAP or CAMEL services.

Example

The following command displays the collected statistics for a MAP service named *MAP-Tewk*.

```
show tcap statistics map-service name MAP-Tewk
```

show temperature

Displays the current temperature on all installed cards. Also displays the temperature of upper and lower fan trays. Temperature readings are acquired from sensors located on theses components.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show temperature [verbose] [| { grep *grep_options* **| more }]**

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

verbose

Indicates that the output is to contain detailed information.

Usage

Verify current temperature of components in chassis.

Example

```
show temperature

show tempterature verbose
```

show terminal

Displays the current terminal settings for number of lines in length and number of characters in width.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show terminal [| { grep *grep_options* **| more }]**

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to verify current terminal settings in case the output displayed appears to have line breaks/wraps in unexpected places.

Example

```
show terminal
```

show threshold

Displays thresholding information for the system.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show threshold [ default ]
```

[default]

Used to display the system's thresholding default values.

Usage

Use this command to display information on threshold value configuration and activity.

Example

The following command displays configuration information pertaining to threshold values configured on the system:

```
show threshold
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show timing

Displays the information configured to define a transmit timing source other than the system clock. The display includes related information (such as port status, timing source priority, timing alarms, etc.) for all of the ports configured for either Building Integrated Timing Supply (BITS) or line timing.

Product

SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show timing
```

Usage

Use this command to determine which line cards are recovering receive timing clocks.

Important: This command is not supported on all platforms.

Example

The following command displays timing configuration and status information for the timing-configured ports.

```
show timing
```

show upgrade

Displays the status of an on-going on-line software upgrade.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

```
show upgrade
```

Usage

Use this command to show the status of an on-going on-line software upgrade.

Important: This command is not supported on all platforms.

show url-blacklisting database

Displays URL Blacklisting static database configurations.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show url-blacklisting database [all | url *url* **| facility acsmgr { all | instance** *instance* **}] [| { grep** *grep_options* **| more }]**

all

Displays configurations of all URL Blacklisting databases present in the default or override directory.

facility acsmgr { all | instance *instance* **}**

Displays configurations of URL Blacklisting database configuration per facility/ACSMgr instance.
all: Displays URL Blacklisting database configuration of all ACSMgrs.
instance *instance*: Displays URL Blacklisting database configuration for the instance number of the database specified as an integer from 1 through 10000000.

url *url*

Displays configurations of the URL Blacklisting database specified in the database's URL expressed as an alphanumeric string of 1 through 512 characters.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view configurations associated with in-memory and on-flash Blacklisting database. The **show url-blacklisting database** command displays the active database that is loaded, and is the one set by either the default or override CLI commands.

Example

The following command displays configurations of all the databases present in default or override directory, indicating one as Active and rest as Not Loaded:

```
show url-blacklisting database all
```

The following command displays configurations of the */flash/bl/optblk.bin* database:

```
show url-blacklisting database url /flash/bl/optblk.bin
```

The following command displays database configuration for the ACSMgr instance *1*:

```
show url-blacklisting database facility acsmgr instance 1
```

Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

show version

Displays the version information for the current system image or for a remote image.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Syntax

show version [*url* **] [all | verbose] [| { grep** *grep_options* **| more }]**

url

Specifies the location of a configuration file for which to display version information. The *url* may refer to a local or a remote file and must be entered in the following format:
[file:] { /flash | /pcmcia1 | /hd } [/*directory* **] /***file_name*
tftp:// { *host* **[** *:port#* **] } [/***directory* **] /***file_name*
[http: | ftp: | sftp:] // [*username* **[** *:password* **] @] {** *host* **} [** *:port#* **] [/***directory* **] /***file_name*

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

all | verbose

all: displays all image information.
verbose: displays detailed information.
The **verbose** keyword may not be used in conjunction with a URL specification.

| { grep *grep_options* **| more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage

Display the version information to verify the image versions loaded in preparation for maintenance, upgrades, etc.

Important: This command is not supported on all platforms.

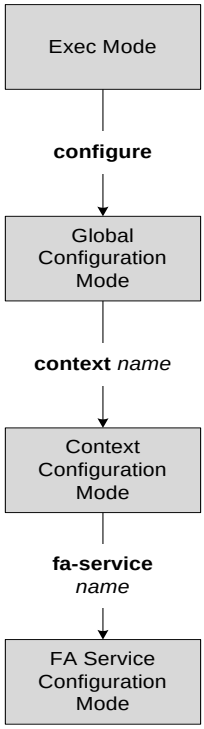
Example

The following commands display the version information with the basic level of output and the detailed level, respectively.

```
show version

show version verbose
```

Chapter 120
FA Service Configuration Mode Commands

The Foreign Agent Service Configuration Mode is used to create and manage the Foreign Agent (FA) services associated with the current context.



advertise

Configures agent advertisement parameters within the FA service.

Product

PDSN, GGSN, ASN GW

Privilege

Security Administrator, Administrator

Syntax

advertise {adv-delay *seconds* |**adv-lifetime** *time* | **adv-interval** { *seconds* | **msec** *num* } | **num-adv-sent** *number* | **prefix-length-extn** | **reg-lifetime** *reg_time* }

no advertise{ **prefix-length-extn** | **reg-lifetime** }

[default] advertise adv-delay

no advertise prefix-length-extn

Disables prefix-length-extn

no advertise reg-lifetime

Specifies that there is no limit to the registration lifetime that the FA service will allow in any Registration Request message from the mobile node.

default advertise adv-delay

Sets the initial delay for the unsolicited advertisement to the default value of 1000 ms.

advertise adv-delay *seconds*

Default: 1000
Sets the initial delay for the unsolicited advertisement.
seconds is the advertisement delay in milliseconds and must be an integer from 10 through 5000.

Important: This command is available for WiMAX CMIP calls only.

adv-lifetime *time*

Default: 9000
Specifies the FA agent advertisement lifetime.
The agent advertisement lifetime is the amount of time that an FA agent advertisement remains valid in the absence of further advertisements.
time is measured in seconds and can be configured to an integer from 1 through 65535.

adv-interval { *seconds* | msec *num* }

Default: 5 seconds
Specifies the amount of time between agent advertisements.
seconds is the time in seconds and can be an integer from 1 through1800.

msec *num*: Configures agent advertisement Interval in milliseconds. *num* can be an integer from 100 through 1800000.

num-adv-sent *number*

Default: 5
Specifies the number of unanswered agent advertisements that the FA service sends upon PPP establishment before rejecting the session.
number can be an integer from 1 through 65535.

prefix-length-extn

Default: Disabled
When enabled, the FA includes the FA-service address in the Router Address field of the Agent Advertisement and appends a Prefix Length Extension in Agent Advertisements with a prefix length of 32.

reg-lifetime *reg_time*

Default: 600
Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node.
reg_time is measured in seconds and can be configured to an integer from 1 through 65534.

Usage

Use to tailor FA advertisements to meet your network needs and/or conditions.

Example

The following command configures the FA advertisement interval at 10 seconds, the advertise lifetime to *20000* seconds, and the maximum number of unanswered advertisements that will be set to *3*.

```
advertise adv-interval 10 adv-lifetime 20000 num-adv-sent 3
```

authentication aaa

This configuration enables or disables the authentication parameters for the FA service to override dynamic keys from AAA with static keys to support MIP registration with an HA that does not support dynamic keys.

Product

FA, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] authentication aaa-distributed-mip-keys override
```

no

Disable the override of dynamic keys from AAA.

default

By default the override behavior is disabled and the system uses dynamic keys from AAA after successful EAP authentication. If EAP authentication fails, the system uses static keys by default.

Usage

Specify how the system will perform authentication of registration request messages. By default dynamic MN-HA and FA-HA keys from AAA after successful EAP authentication used by a PMIP client in WiMAX calls for MIP registration with HA. This configuration in FA service overrides the dynamic keys from AAA with static keys to support MIP registration with an HA that does not support dynamic keys.

Example

The following command configures the FA service to override use of AAA MIP keys and force the use of statically configured FA-HA SPI/key for WiMAX calls.

```
authentication aaa-distributed-mip-keys override
```

authentication mn-aaa

Specifies how the system handles authentication for mobile node re-registrations.

Product

PDSN, ASN GW, GGS

Privilege

Security Administrator, Administrator

Syntax

```
authentication mn-aaa { always | ignore-after-handoff | init-reg | init-reg-except-
handoff | renew-and-dereg-noauth | renew-reg-noauth } [ optimize-retries ]
```

always

Specifies that the FA service performs authentication each time a mobile node registers. This is the default setting.

ignore-after-handoff

MN-AAA authentication is not done at the FA for a handoff Access Gateway (AGW).

init-reg

MN-AAA and MN-FAC extensions are required only in initialization RRQ.

init-reg-except-handoff

MN-AAA and MN-FAC extensions are not required in initialization RRQ after inter-Access Gateway (AGW) handoff.

renew-and-dereg-noauth

Specifies that the FA service does not perform authentication for mobile node re-registration or deregistration authorization requests. Initial registration is handled normally.

renew-reg-noauth

Specifies that the FA service does not perform authentication for mobile node re-registrations. Initial registration and de-registration are handled normally.

optimize-retries

Optimizes the number of Authentication retries sent to the AAA server.
When an authentication request is pending for a MIP call at the AGW, if a retry RRQ is received from the mobile node, the AGW discards the old RRQ and keeps the most recent RRQ. Subsequently when the authentication succeeds, the AGW forwards the most recent RRQ to the HA. If the authentication fails, the AGW replies to the MN using the most recent RRQ.

Usage

Use this command to determine how the FA service handles mobile node re-registrations.
The system is shipped from the factory with the mobile AAA authentication set to always.

Example

The following command configures the configures the FA service to perform mobile node authentication for every re-registration:

```
authentication mn-aaa always
```

The following command specifies that the FA service does not perform authentication for mobile node re-registrations:

```
authentication mn-aaa renew-reg-noauth
```

authentication mn-ha

Configures whether the FA service looks for a Mobile Network-Home Agent (MN-HA) authentication extension in the RRP (registration reply).

Product

PDSN, ASN GW, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
authentication mn-ha { allow-noauth | always }
```

allow-noauth

Allows a reply that does not contain the auth extension.

always

A reply should always contain the auth extension to be accepted.
This is the default setting.

Usage

Use this command to determine whether or not the FA service requires the MN-HA auth extension in the RRP.
The system is shipped from the factory with this set to always.

Example

The following command configures the FA service to require a reply to contain the authentication extension to be accepted.:

```
authentication mn-ha always
```

bind

Binds the FA service to a logical IP interface serving as the Pi interface and specifies the maximum number of subscribers that can access this service over the interface.

Product

PDSN, ASN GW, GGSN PDIF

Privilege

Security Administrator, Administrator

Syntax

bind address *address* [**max-subscribers** *count*]

no bind address

address

Specifies the IP address (address) of the interface configured as the Pi interface. *address* is specified in IPv4 dotted-decimal notation.

max-subscribers *max#*

Default: 500000
Specifies the maximum number of subscribers that can access this service on this interface.
count can be configured to an integer from 0 through 500000.

Important: The maximum number of subscribers supported is dependant on the license key installed and the number of active packet processing cards installed in the system. Refer to the license key command for additional information.

Usage

Associate or tie the FA service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an Pi interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.
This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.
When configuring the **max-subscribers** option, be sure to consider the following:

- The total number of interfaces you will configure for use as Pi interfaces
- The maximum number of subscriber sessions that all of these interfaces may handle during peak busy hours
- The average bandwidth for each of the sessions
- The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.
Use the **no bind address** command to delete a previously configured binding.

Example

The following command would bind the logical IP interface with the address of *192.168.3.1* to the FA service and specifies that a maximum of *600* simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```
bind address 192.168.3.1 max-subscribers 600
```

The following command disables a binding that was previously configured:

```
no bind address
```

challenge-window

Defines the number of recently sent challenge values that are considered valid by the FA.

Product

PDSN, ASN GW, GGSN

Privilege

Security Administrator, Administrator

Syntax

challenge-window *number*

number

Default: 2
The number of recently sent challenge values that are considered valid. *number* must be an integer from 1 through 5.

Usage

Use this command to set the number of recently sent challenge values that are considered valid by the FA.

Example

Set the challenge window to *3*:

```
challenge-window 3
```

default subscriber

Specifies the name of a subscriber profile configured within the same context as the FA service from which to base the handling of all other subscriber sessions handled by the FA service.

Product

PDSN, ASN GW, GGSN PDIF

Privilege

Security Administrator, Administrator

Syntax

default subscriber *profile_name*

no default subscriber *profile_name*

profile_name

Specifies the name of the configured subscriber profile. *profile_name* is an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage

Each subscriber profile specifies "rules" such as permissions, PPP settings, and timeout values.
By default, the FA service will use the information configured for the subscriber named default within the same context. This command allows for multiple FA services within the same context to apply different "rules" to sessions they process. Each set of rules can be configured under a different subscriber name which is pointed to by this command.
Use the **no default subscriber** *profile_name* command to delete the configured default subscriber.

Example

To configure the FA service to apply the rules configured for a subscriber named *user1* to every other subscriber session it processes, enter the following command:

```
default subscriber user1
```

dynamic-ha-assignment

This command configures various dynamic HA assignment parameters.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] dynamic-ha-assignment [ aaa-override mn-supplied-ha-addr | allow-failover ]
```

default

Feature is disabled by default.

no

Removes the feature and returns it to the default setting of disabled.

aaa-override mn-supplied-ha-addr

Enables the system to override the mobile node supplied HA IP address with the AAA provided HA address.

allow-failover

Enables/disables a failover retry for dynamic HA assignment from the AAA server.

Usage

Use this command to override the mobile node supplied HA IP address with the AAA supplied HA address. Use this command to enable or disable the failover feature that allows the system to receive and use a newer HA address from the AAA server in cases where the original HA address is not responding.
A AAA server may assign different HA addresses each time a retransmitted MIP RRQ is authenticated during the MIP session setup. When this configuration is enabled, if the FA gets a new HA address from AAA during setup, it discards the previous HA address and start using the new address. This allows the FA session to connect to an available HA during setup.

Example

The following command enables the failover feature that allows the system to receive and use a newer HA address from the AAA server:

```
dynamic-ha-assignment allow-failover
```

dynamic-mip-key-update

When enabled, the FA service processes MIP_Key_Update_Request from the AAA server and allows dynamic MIP key updates (DMUs).

Default: Disabled

Product

PDSN, ASN GW, GGSN

Privilege

Security Administrator, Administrator

Syntax

dynamic-mip-key-update

no dynamic-mip-key-update

no

The FA service rejects MIP_Key_Update_Request from the AAA server, not allowing dynamic MIP key updating to occur and terminates the call.

Usage

Use this command to enable or disable the DMU feature in the FA service.

Example

To enable DMU and allow dynamic updates of MIP keys, enter the following command:

```
dynamic-mip-key-update
```

encapsulation allow gre

Enables or disables the use of generic routing encapsulation (GRE) when establishing a Mobile IP (MIP) session. When enabled, if requested by a Mobile Node (MN), the FA requests the HA to use GRE encapsulation when establishing the MIP session. When disabled, the FA does not set the GRE bit in Agent Advertisements to the MN.

Default: GRE is enabled.

Product

PDSN, ASN GW, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
encapsulation allow gre

no encapsulation allow gre
```

Usage

Use to disable or re-enable the use of GRE encapsulation for MIP sessions.

Example

To re-enable GRE encapsulation for MIP sessions, enter the following command:

```
encapsulation allow gre
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

fa-ha-spi

Configures the security parameter index (SPI) between the FA service and the HA.

Product

PDSN, ASN GW, GGSN PDIF

Privilege

Security Administrator, Administrator

Syntax

fa-ha-spi remote-address { *ha_ip_address* | *ip_addr_mask_combo* } **spi-number** *number* { **encrypted secret** *enc_secret* | *secret* } [**description string** | **hash-algorithm** { **hmac-md5** | **md5** | **rfc2002-md5** } | **monitor-ha** | **replay-protection** { **timestamp** | **nonce** } | **timestamp-tolerance** *tolerance* **]**

no fa-ha-spi remote-address { *ha_ip_address* | *ip_addr_mask_combo* } **spi-number** *number*

remote-address { *ha_ip_address* | *ip_addr_mask_combo* }

ha_ip_address: Specifies the IP address of the HA in IPv4 dotted-decimal notation.
ip_addr_mask_combo: Specifies the IP address of the HA including network mask bits.
ip_addr_mask_combo must be specified IPv4 dotted-decimal notation with CIDR subnet mask bits (x.x.x.x/xx).

spi-number *number*

Specifies the Security Parameter Index (SPI) which indicates a security context between the FA and the HA in accordance with RFC 2002.
number can be configured to an integer from 256 through 4294967295.

encrypted secret *enc_secret* **| secret** *secret*

Configures the shared-secret between the FA service and the HA. The secret can be either encrypted or non-encrypted.

- **encrypted secret** *enc_secret* : Specifies the encrypted shared key (enc_secret) between the FA service and the HA. *enc_secret* must be an alphanumeric string of 1 through 254 characters that is case sensitive.

Important: The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

- **secret** *secret*: Specifies the shared key (secret) between the FA service and the HA. *secret* must be an alphanumeric string of 1 through 127 characters that is case sensitive.

description *string*

This is a description for the SPI. *string* must be an alphanumeric string of 1 through 31 characters.

hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }

Default: hmac-md5
Specifies the hash-algorithm used between the FA service and the HA.

- **hmac-md5**: Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis.
- **md5**: Configures the hash-algorithm to implement MD5 per RFC 1321.
- **rfc2002-md5**: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

monitor-ha

Default: disabled
Enables the HA monitor feature for this HA address.
To set the behavior of the HA monitor feature, refer to the **ha-monitor** command in this chapter. To disable this command (if enabled) for this HA address, re-enter the entire **fa-ha-spi** command without the **monitor-ha** keyword.

replay-protection { timestamp | nonce }

Default: timestamp
Specifies the replay-protection scheme that should be implemented by the FA service for this SPI.

- **nonce**: Configures replay protection to be implemented using NONCE per RFC 2002. Nonce is an arbitrary number used only once to sign a cryptographic communication.
- **timestamp**: Configures replay protection to be implemented using timestamps per RFC 2002.

Important: This keyword should only be used in conjunction with Proxy Mobile IP support.

timestamp-tolerance *tolerance*

Default: 60
Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. If this is set to 0, then timestamp tolerance checking is disabled at the receiving end.
tolerance is measured in seconds and can be configured to an integer value from 0 through 65535.

Important: This keyword should only be used in conjunction with Proxy Mobile IP support.

+

More than one of the above keywords can be entered within a single command.

Usage

An SPI is a security mechanism configured and shared by the FA service and the HA. Please refer to RFC 2002 for additional information.
Though it is possible for FAs and HAs to communicate without SPIs being configured, the use of them is recommended for security purposes. It is also recommended that a “default” SPI with a remote address of 0.0.0.0/0 be configured on both the HA and FA to prevent hackers from spoofing addresses.

Important: The SPI configuration on the HA must match the SPI configuration for the FA service on the system in order for the two devices to communicate properly.

A maximum of 2,048 SPIs can be configured per FA service.
Use the **no** version of this command to delete a previously configured SPI.

Example

The following command configures the FA service to use an SPI of *512* when communicating with an HA with the IP address *192.168.0.2*. The key that would be shared between the HA and the FA service is *q397F65*. When communicating with this HA, the FA service will also be configured to use the *rfc2002-md5* hash-algorithm.

```
fa-ha-spi remote-address 192.168.0.2 spi-number 512 secret q397F65 hash-
algorithm rfc2002-md5
```

The following command deletes the configured SPI of *400* for an HA with an IP address of *172.100.3.200*:

```
no fa-ha-spi remote-address 172.100.3.200 spi-number 400
```

gre

Configures Generic Routing Encapsulation (GRE) parameters.

Product

PDSN, ASN GW, GGSN

Privilege

Security Administrator, Administrator

Syntax

gre { checksum | checksum-verify | reorder-timeout *timeout* **| sequence-mode { none | reorder } | sequence-numbers }**

no gre { checksum | checksum-verify | sequence-numbers }

no

Disables the specified functionality.

checksum

Default: disabled
Enables the introduction of the checksum field in outgoing GRE packets.

checksum-verify

Default: disabled
Enables verification of the GRE checksum (if present) in incoming GRE packets.

reorder-timeout *timeout*

Default: 100
Configures maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets. *timeout* must be an integer from 0 through 5000.

sequence-mode { none | reorder }

Default: none
Configures how incoming out-of-sequence GRE packets should be handled.
none: Disables reordering of incoming out-of-sequence GRE packets.
reorder: Enables reordering of incoming out-of-sequence GRE packets.

sequence-numbers

Default: Disabled.
Enables insertion or removal of GRE sequence numbers in GRE packets.

Usage

Use this command to configure how the FA service handles GRE packets.

Example

To set maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets to *500* milliseconds, enter the following command:

```
gre reorder-timeout 500
```

To enable the reordering of incoming out of sequence GRE packets, enter the following command:

```
gre sequence-mode reorder
```

ha-monitor

Configures the behavior of the HA monitor feature.

Product

PDSN, ASN GW, FA, HA

Privilege

Security Administrator, Administrator

Syntax

[default] ha-monitor [interval *sec*| **max-inactivity-time** *sec* | **num-retry** *num* **]**

no ha-monitor

default

Restores the system default setting(s) for the command/keyword(s). This command is disabled by default.

no

Disables the HA monitoring feature for this FA service.

interval *sec*

Default: 30
Configures the time interval before the next monitoring request message is sent to the HA.
sec must be an integer from 1 through 36000.

max-inactivity-time *sec*

Default: 60
Specifies the maximum amount of time the system will wait without receiving MIP control traffic from a HA before the HA monitoring mechanism is triggered.
sec must be an integer from 30 through 600.

num-retry *num*

Default: 5
Configures the number of time the system will attempt to send HA monitor requests before determining the HA is down and a trap is initiated.
num must be an integer from 0 through 10.

Usage

Use this command to set parameters for the HA monitor feature. This feature allows the AGW/FA to monitor HAs with which it has MIP sessions. The monitoring feature is triggered when the AGW/FA does not receive any MIP traffic from a HA for a configured amount of time (**max-inactivity-time**). The AGW/FA starts sending special MIP RRQ monitor messages and waits for RRP monitor message responses from the HA. The RRQ monitor messages are addressed to the HA service address. The source address of the monitor-request messages is the FA service's IP address.
The actions taken during monitoring are comprised of the following:

- If no monitor response is received during the interval time (**interval**), the AGW retransmits the monitor message a configured number of times (**num-retry**).
- If no response is received after retransmitting for the number configured in **num-retry**, the HA is considered down. The AGW/FA sends a trap (HAUnreachable) to the management station. Monitoring of this HA is stopped until a MIP control message is received from the particular HA and when the AGW/FA sends a trap (HAreachable) to the management station and starts monitoring the HA again.
- When an HA receives the RRQ from an FA, it verifies the message and identifies it as a monitor message based on a special reserved NAI (in the message) and a Monitor HA CVSE in the RRQ. The HA responds with an RRP with Reply code 0x00 (accepted) and includes the Monitor HA CVSE. When the FA receives the RRP from the HA, it updates the activity for the peer HA to maintain the "up" state.

Important: This command only sets the behavior of the HA monitor feature. To enable the HA monitor feature for each HA address, refer to the **fa-ha-spi** command in this chapter. Up to 256 HAs can be monitored per system.

Example

The following commands set the HA monitor message interval to *45* seconds, the HA inactivity time to *60* seconds, and the number of HA monitor retries to *6*:

```
ha-monitor interval 45ha-monitor max-inactivity-time 60ha-monitor num-
retry 6
```

idle-timeout-mode

Controls whether Mobile IP data and control packets or only Mobile IP data resets the session idle timer.

Product

PDSN, ASN GW, GGSN PDIF

Privilege

Security Administrator, Administrator

Syntax

```
idle-timeout-mode {aggressive | normal}
```

aggressive

Only Mobile IP data resets the session idle timer.

normal

Both Mobile IP data and control packets reset the session idle timer.

Usage

Use this command to control how the session idle timer is reset.

Example

The following command specifies that only Mobile IP data can reset the session idle timer:

```
idle-timeout-mode aggressive
```

ignore-mip-key-data

When this command is enabled, if the Dynamic Mobile IP Key Update (DMU) is not enabled and the mobile node (MN) sends a MIP_Key_Data CVSE, the FA ignores the MIP_Key_Data extension and the call is continued like a regular Mobile IP (MIP) call.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

ignore-mip-key-data

no ignore-mip-key-data

no

Disable ignoring of MIP key data.

Usage

When DMU is not enabled, use this command to ignore MIP key data sent by the MN and allow the call to continue normally.

Example

To enable the FA to ignore MIP key data sent by the MN, enter the following command:

```
ignore-mip-key-data
```

ignore-stale-challenge

Enables the system to accept RRQs with previously used challenges. This feature is disabled by default.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
ignore-stale-challenge

no ignore-stale-challenge
```

no

Disables this feature. If an RRQ is received with a previously used challenge and there are RRQs pending on the same session, accept the RRQ if it has a new Identification in the retransmitted RRQ. All other RRQs received with previously used challenge are rejected with the Stale Challenge (106) error code.

Usage

Use this command to allow the FA to accept stale challenges regardless of the ID field or if other RRQs are pending.

Example

To enable this functionality in the FA service, enter the following command;

```
ignore-stale-challenge
```

To disable this functionality, enter the following command;

```
no ignore-stale-challenge
```

ip local-port

Configures the local User Datagram Protocol (UDP) port for the Pi interfaces' IP socket on which to listen for Mobile IP Registration messages.

Product

PDSN, ASN GW, GGSN

Privilege

Security Administrator, Administrator

Syntax

ip local-port *port#*

port#

Specifies the UDP port number.
port# can be an integer from 1 through 65535.

Usage

Specify the UDP port that should be used for communications between the FA service and the HA. The system defaults to using local port 434.

Example

The following command specifies a UDP port of *3950* for FA-to-HA communication on the Pi interface:

```
ip local-port 3950
```

isakmp

Configures support for IPSec within the FA-service.

Product

PDSN, ASN GW, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
isakmp {peer-ha ha_address {crypto map map_name [ [ encrypted ] secret secret ]} |
default { crypto map map_name [ [ encrypted ] secretsecret]}}

no isakmp { peer-ha peer_ip_address | default }
```

---

no

Deletes the reference to the crypto map for the specified HA, or deletes the reference for the default crypto map.

---

peer-ha *ha_address* **{ crypto map** *map_name* **[[encrypted] secret** *preshared_secret* **] }**

Configures a crypto map for a peer HA.

- *ha_address*: The IP address of the HA with which the FA service will establish an IPSec SA. The address must be expressed in IPv4 dotted-decimal format.
- **crypto map** *map_name*: The name of a crypto map configured in the same context that defines the IPSec tunnel properties. *map_name* is the name of the crypto map expressed as an alphanumeric string of 1 through 127 characters.
- **encrypted**: This keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.
- **secret** *secret*: The pre-shared secret that will be used during the IKE negotiation. *preshared_secret* is the secret expressed as an alphanumeric string of 1 through 127 characters.

---

default { crypto map *map_name* **[[encrypted] secret** *secret* **] }**

Specifies the default crypto map to use when there is no matching crypto map configured for an HA address.

- **crypto map** *map_name*: The name of a crypto map configured in the same context that defines the IPSec tunnel properties. *map_name* is the name of the crypto map expressed as an alphanumeric string of 1 through 127 characters.
- **encrypted**: This keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.
- **secret** *secret*: The pre-shared secret that will be used during the IKE negotiation. *preshared_secret* is the secret expressed as an alphanumeric string of 1 through 127 characters.

Usage

Use this command to configure the FA-service's per-HA IPSec parameters. These dictate how the FA service is to establish an IPSec SA with the specified HA.

Important: For maximum security, the above command should be executed for every possible HA with which the FA service communicates.

A default crypto map can also be configured using the default keyword. The default crypto map is used in the event that the AAA server returns an HA address that is not configured as an isakmp peer-ha.

Important: For maximum security, the default crypto map should be configured in addition to peer-ha crypto maps instead of being used to provide IPSec SAs to all HAs.

Note that once an IPSec tunnel is established between the FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the tunnel regardless of whether or not IPSec is supported for the new subscriber sessions. Data for existing Mobile IP sessions is unaffected.

Example

The following command creates a reference for an HA with the IP address *10.2.3.4* to a crypto map named *map1*:

```
isakmp peer-ha 10.2.3.4 crypto map map1
```

The following command deletes the crypto map reference for the HA with the IP address *10.2.3.4*.

```
no isakmp peer-ha 10.2.3.4
```

limit-reg-lifetime

Enable the current default behavior of limiting the Mobile IP (MIP) lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts. When disabled, this command allows a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.

Product

PDSN, ASN GW, GGSN PDIF

Privilege

Security Administrator, Administrator

Syntax

```
[no | default] limit-reg-lifetime
```

no

Allows a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.

default

Enables the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts.

Usage

Use the no keyword with this command to allow a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.
Use the base command or the keyword to reset the FA service to the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts.

Example

Configure the FA service to allow a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts by entering the following command:
no limit-reg-lifetime
Configure the FA service to the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts by entering either of the following commands:

default limit-reg-lifetimelimit-reg-lifetime

max-challenge-len

For mobile subscribers, the FA generates a random number and sends it to the mobile node as part of the mobile authentication extension (Mobile-Foreign Authentication extension) as described in RFC 3012. This command sets the maximum length of the FA challenge in bytes.

Product

PDSN, ASN GW, GGSN

Privilege

Security Administrator, Administrator

Syntax

max-challenge-len *length*

length

Default: 16
The maximum length, in bytes, of the FA challenge. This value must be an integer from 4 through 32.

Usage

Change the maximum allowed length of the randomly generated FA challenge its default of 16.

Example

Use the following command to change the maximum length of the FA challenge to 18 bytes:

```
max-challenge-len 18
```

mn-aaa-removal-indication

Enables the FA to remove the Mobile Network-Final Assembly Code (MN-FAC) and MN-AAA extensions from RRQs. This is disabled by default.

Product

PDSN, ASN GW, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
mn-aaa-removal-indication

no mn-aaa-removal-indication
```

no

Disable the removal of the MN-FAC and MN-AAA extensions from RRQs.

Usage

Enable this feature if there is no need to authenticate the subscriber at HA using MN-AAA extension.

Example

The following command enables the FA service to remove MN-FAC and MN-AAA extensions from RRQs:

```
mn-aaa-removal-indication
```

multiple-reg

Specifies the number of simultaneous Mobile IP sessions that will be supported for over a single PPP session.

Product

PDSN, ASN GW, GGSN

Privilege

Security Administrator, Administrator

Syntax

multiple-reg *number*

number

number can be configured to an integer from 1 through 3.

Usage

Use to support multiple registrations per subscriber.
The system defaults to a setting of "1" for multiple simultaneous MIP sessions.

Important: The system will only support multiple Mobile IP sessions per subscriber if the subscriber's mobile node has a static IP address. The system will only allow a single Mobile IP session for mobile nodes that receive a dynamically assigned IP address. In addition, because only a single Mobile IP or proxy-Mobile IP session is supported for IP PDP contexts, this parameter must remain at its default configuration.

Example

The following command configures the number of supported simultaneous registrations for subscribers using this FA service to *3*.

```
multiple-reg 3
```

optimize tunnel-reassembly

Configures FA to HA optimization for tunnel reassembly.

Product

PDSN, ASN GW, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
optimize tunnel-reassembly

no optimize tunnel-reassembly
```

Usage

Enabling this functionality fragments large packets prior to encapsulation for easier processing. Tunnel reassembly optimization is disabled by default.

Important: You should not use this command without first consulting Cisco Systems Technical Support. This command applies to very specific scenarios where packet reassembly is not supported at the far end of the tunnel. There are cases where the destination network may either discard the data, or be unable to reassemble the packets.

Important: This functionality works best when the FA service is communicating with an HA service running in a system. However, an FA service running in the system communicating with an HA from a different manufacturer will operate correctly even if this parameter is enabled.

Use the **no** version of this command to disable tunnel optimization if it was previously enabled.

Example

The following command enables tunnel reassembly optimization:

```
optimize tunnel-reassembly
```

private-address allow-no-reverse-tunnel

This command enables the FA to allow calls with private addresses and no reverse tunneling.

Product

PDSN, ASN GW, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
private-address allow-no-reverse-tunnel

no private-address allow-no-reverse-tunnel
```

no

Disables the functionality. This is the default setting.

Usage

Use this command to let the FA allow sessions with private addresses that do not have the reverse tunnel bit set.

Example

To enable sessions with private addresses and no reverse tunneling, enter the following command:

```
private-address allow-no-reverse-tunnel
```

proxy-mip

Configures parameters pertaining to Proxy Mobile IP support.

Product

PDSN, ASN GW, GGSN PDIF

Privilege

Security Administrator, Administrator

Syntax

proxy-mip { allow | ha-failover [max-attempts *max_attempts* **| num-attempts-before-switching** *num_attempts* **| timeout seconds]| max-retransmissions number | renew-percent-time** *renew-time* **| retransmission-timeout** *time* **}**

```
no proxy-mip {allow | ha-failover }
```

```
default proxy-mip {allow | ha-failover | max-retransmissions | renew-percent-time |
retransmission-timeout}
```

no

Disables FA service support for Proxy Mobile IP or HA failover for Proxy Mobile IP.

default

Restores the specified option to the default setting as described below.

allow

Default: Disabled
Enables FA service support for Proxy Mobile IP.

ha-failover [max-attempts *max_attempts* **| num-attempts-before-switching** *num_attempts* **| timeout** *seconds* **]**

Default: Disabled
Enables HA failover for the Proxy Mobile IP feature.

- **max-attempts** *max_attempts* - Configures the maximum number of retransmissions of Proxy MIP control messages. *max_attempts* must be an integer from 1 through 10. Default is 4
- **num-attempts-before-switching** *num_attempts* - Configures the total number of RRQ attempts (including retransmissions) before failing over to the alternate HA. *num_attempts* must be an integer from 1 through 5. Default is 2.
- **timeout** *seconds* - Configures the retransmission timeout (in seconds) of Proxy MIP control messages when failover happens. *seconds* must be an integer from 1 through 50. Default is 2

max-retransmissions *number*

Default: 5
Configures the maximum number re-try attempts that the FA service is allowed to make when sending Proxy Mobile IP Registration Requests to the HA.
number is the maximum number of retries and can be configured to an integer from 1 through 4294967295.

renew-percent-time *renew-time*

Default: 75
Configures the amount of time that must pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request.
renew-time is entered as a percentage of the advertisement registration lifetime configured for the FA service. (Refer to the **advertise** command in this chapter). *renew-time* can be configured to an integer from 1 through 100.
The following equation can be used to calculate *renew-time*:
renew-time = (duration / lifetime) * 100
duration = The desired amount of time that can pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request
lifetime = The advertisement registration lifetime configured for the FA service.
duration / lifetime

retransmission-timeout *time*

Default: 3
Configures the maximum amount of time allowed by the FA for a response from the HA before re-sending a Proxy Mobile IP Registration Request message.
time is measured in seconds and can be configured to an integer from 1 through 100.

Usage

The **proxy-mip** command and its keywords configure the FA services support for Proxy Mobile IP.
When enabled though the session license and feature use key, the system supports Proxy Mobile IP to provide a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP.
In addition to the parameters configured via this command, the HA-FA SPI(s) must also be modified to support Proxy Mobile IP. Refer to the **fa-ha-spi** command for more information.

Example

The following command configures the FA service to wait up to *5* seconds for an HA to respond prior to re-sending an a Mobile IP Registration Request message:

```
proxy-mip retransmission-timeout 5
```

If the advertisement registration lifetime configured for the FA service is 900 seconds and you want the system to send a Proxy Mobile IP Registration Renewal Request message after 500 seconds, then the following command must be executed:

```
proxy-mip renew-percent-time 50
```

Note that 50 = (450 / 900) 100.

reg-timeout

Configures the FA registration reply timeout.

Product

PDSN, ASN GW, GGSN PDIF

Privilege

Security Administrator, Administrator

Syntax

reg-timeout *time*

time

Default: 45
time is measured in seconds and can be configured to an integer from 1 through 65535.

Usage

Configure the amount of time that the FA service will wait for a Registration Reply from an HA before the call is rejected with a reply code of 78H (registration Timeout).

Example

The following command configures a registration timeout of 10.

```
reg-timeout 10
```

reverse-tunnel

Enables the use of reverse tunneling for a Mobile IP (MIP) sessions when requested by the mobile node (MN).

Product

PDSN, ASN GW, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
reverse-tunnel

no reverse-tunnel
```

no

Indicates the reverse tunnel option is to be disabled. When omitted, the reverse tunnel option is enabled.

Usage

Reverse tunneling involves tunneling datagrams originated by the MN to the HA via the FA service.
When an MN arrives at a foreign network, it listens for agent advertisements and selects an FA that supports reverse tunnels. The MN requests this service when it registers through the selected FA. At this time, the MN may also specify a delivery technique such as Direct or the Encapsulating Delivery Style.
The advantages of using reverse-tunneling:

- All datagrams from the mobile node seem to originate from its home network
- The FA can keep track of the HA that the mobile node is registered to and tunnel all datagrams from the mobile node to its HA

Use the **no** option of this command to disable reverse tunneling. If reverse tunneling is disabled, and the mobile node does not request it, then triangular routing is used.
The system defaults to reverse tunnel enabled.

Important: If reverse tunneling is disabled on the system and an MN requests it, the call will be rejected with a reply code of 74H (reverse-tunneling unavailable).

Example

The following command disables reverse-tunneling support for the FA service:

```
no reverse-tunnel
```

revocation

Enables the MIP revocation feature and configures revocation parameters.

Product

PDSN, ASN GW, GGSN PDIF

Privilege

Security Administrator, Administrator

Syntax

```
revocation { enable | max-retransmission number | negotiate-i-bit | retransmission-
timeout secs | trigger internal-failure }

no revocation enable | trigger internal-failure | negotiate-i-bit
```

no revocation { enable | negotiate-i-bit | trigger internal-failure }

Completely disables registration revocation on the FA.
Disables sending revocation messages to the HA when a session is affected by an internal task failure.

enable

Enables the MIP registration revocation feature on the FA. When enabled, if revocation is negotiated with an HA, and a MIP binding is terminated, the FA can send a Revocation message to the HA. This feature is disabled by default.

max-retransmission *number*

Default: 3
Specifies the maximum number of retransmissions of a Revocation message before the revocation fails. *number* must be an integer from 0 through 10.

negotiate-i-bit

Default: disabled
Enables the FA to negotiate the i-bit via PRQ/RRP messages and processes the i-bit revocation messages.

retransmission-timeout *secs*

Default: 3
Specifies the number of seconds to wait for a Revocation Acknowledgement from the HA before retransmitting the Revocation message. *secs* must be an integer from 1 through 10.

trigger internal-failure

Default: disabled
Enable sending a revocation message to the HA for all sessions that are affected by an internal task failure.

Usage

Use this command to enable or disable the MIP revocation feature on the FA or to change settings for this feature. Both the HA and the FA must have Registration Revocation enabled and FA/HA authorization must be in use for Registration Revocation to be negotiated successfully.

Example

The following command enables Registration Revocation on the FA:

```
revocation enable
```

The following command sets the maximum number of retries for a Revocation message to 6:

```
revocation max-retransmission 6
```

The following command sets the timeout between retransmissions to 10:

```
revocation retransmission-timeout 10
```

threshold reg-reply-error

Set an alarm or alert based on the number of registration reply errors per FA service.

Product

PDSN, ASN GW, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
threshold reg-reply-error high_thresh [ clear low_thresh ]

no threshold reg-reply-error
```

no

Deletes the alert or alarm.

high_thresh

Default: 0
The high threshold number of registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* can be an integer from 0 through 100000.

Important: You must enter a value between 1 and 100000 to trigger an alert/alarm.

clear *low_thresh*

Default:0
The low threshold number of registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. *low_thresh* can be an integer from 0 through 100000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Important: You must enter a value between 1 and 100000 to trigger an alert/alarm.

Usage

Use this command to set an alert or an alarm when the number of registration reply errors is equal to or greater than a specified number of calls per second.
Alerts or alarms are triggered for the number of registration reply errors on the following rules:

- **Enter condition**: Actual number of registration reply errors > High Threshold
- **Clear condition**: Actual number of registration reply errors £ Low Threshold

Example

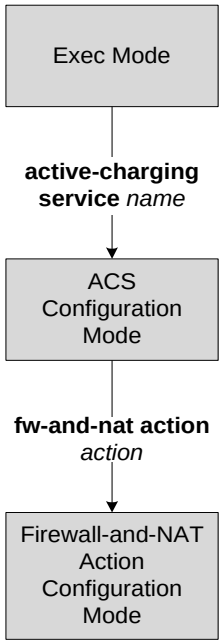
The following command configures a registration reply error threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold reg-reply-error 1000 clear 500
```

Chapter 121
Firewall-and-NAT Action Configuration Mode Commands

The Firewall-and-NAT Action Configuration Mode enables configuring Stateful Firewall (FW) and Network Address Translation (NAT) actions.

Important: This configuration mode is only available in release 11.0 and later releases. This configuration mode must be used to configure Action-based Stateful Firewall and NAT features.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

flow check-point

This command checkpoints all the flows matching the Firewall-and NAT action.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

flow check-point [data-usage *data_usage* **[and | or] | time-duration** *duration* **[and | or]]**

{ default | no } flow check-point

default

Configures the default Firewall action.

no

Deletes the Firewall action configuration.

data-usage *data_usage*

Specifies the data usage in bytes.
data_usage must be an integer from 1 through 4294967295.
The maximum limit for data-usage is 4 GB.

time-duration *duration*

Specifies the time duration in seconds.
duration must be an integer from 1 through 86400.
The maximum limit for time-duration is 24 hours.

and | or

This option allows to configure only **data-usage** or **time-duration**, or a combination of **data-usage** and **time-duration**.

Usage

Use this command to enable/disable the check-pointing of NATed flows and control the type of flows need to be check pointed based on specified criteria. Check pointing is done only for TCP and UDP flows.

Example

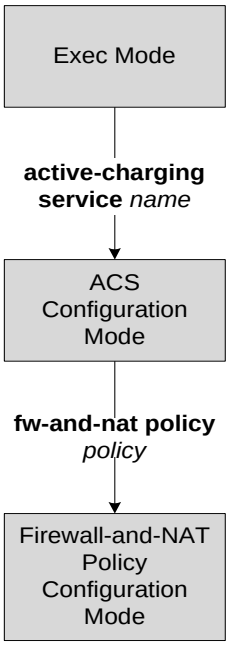
The following command configures Stateful Firewall to drop packets with data-usage *5000*:

```
flow check-point data-usage 5000
```

Chapter 122
Firewall-and-NAT Policy Configuration Mode Commands

The Firewall-and-NAT Policy Configuration Mode enables configuring Stateful Firewall (FW) and Network Address Translation (NAT) policies.

Important: This configuration mode is only available in 8.1, 9.0, and later releases. This configuration mode must be used to configure Policy-based Stateful Firewall and NAT features.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

access-rule

This command creates and configures an access rule.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

access-rule { no-ruledef-matches { downlink | uplink } action { deny [charging-action *charging_action* **] | permit [bypass-nat | nat-realm** *nat_realm* **[fw-and-nat-action** *name* **]] } | priority** *priority* **{ [dynamic-only | static-and-dynamic] access-ruledef** *ruledef_name* **{ deny [charging-action** *charging_action* **] | permit [[bypass-nat | nat-realm** *nat_realm* **[fw-and-nat-action** *name* **]] | trigger open-port {** *port_number* **| range** *start_port* **to** *end_port* **} direction { both | reverse | same }] } } }**

default access-rule no-ruledef-matches { downlink | uplink } action

no access-rule priority *priority*

default

Configures the default setting.
Default: Uplink direction: **permit**; Downlink direction: **deny**

no

Removes the access rule specified by the priority.

no-ruledef-matches

Configures action on packets with no ruledef match.

downlink

Specifies to act on downlink packets with no ruledef match.

uplink

Specifies to act on uplink packets with no ruledef match.

action

Specifies action to take on downlink/uplink packets with no ruledef match.

deny

Specifies to deny packets.

permit

Specifies to permit packets and allow the creation of data flows.

charging-action *charging_action*

Specifies the charging action. Optionally, a charging action can be configured for deny action. If a packet matches the deny rule, action is taken as configured in the charging action. If a charging action is specified, the content-ID and billing-action configured in the charging action are used. Also, the flow may be terminated (instead of just discarding the packet), if so configured in the specified charging action.
charging_action must be an alphanumeric string of 1 through 63 characters.

bypass-nat

Important: In 9.0 and later releases, this keyword is NAT license dependent.

Specifies to bypass NAT.

nat-realm *nat_realm*

Important: In 9.0 and later releases, this keyword is NAT license dependent.

Specifies the NAT realm to be used to perform NAT on subscriber packets matching the access ruledef. If the NAT realm is not specified, NAT will be bypassed. That is, NAT will not be performed on subscriber packets that are matching a ruledef with no NAT realm name configured in it.
nat_realm must be an alphanumeric string of 1 through 31 characters.

priority *priority*

Specifies priority of an access ruledef in the Firewall-and-NAT policy.
priority must be an integer from 1 through 65535 that is unique for each access ruledef in the Firewall-and-NAT policy.

[dynamic-only | static-and-dynamic] access-ruledef *ruledef_name*

Specifies the access ruledef name. Optionally, the ruledef type can also be specified.

- **dynamic-only**: Dynamic Ruledef—Predefined ruledef that can be enabled/disabled by the policy server, and is disabled by default.
- **static-and-dynamic**: Static and Dynamic Ruledef—Predefined ruledef that can be enabled/disabled by the policy server, and is enabled by default.
- **access-ruledef** *ruledef_name*: Specifies the access ruledef name. *ruledef_name* must be an alphanumeric string of 1 through 63 characters.

trigger open-port { *port_number* | range *start_port* to *end_port* } direction { both | reverse | same }

Important: In 9.0 and later releases, this keyword is Stateful Firewall license dependent.

Optionally a port trigger can be specified to be used for this rule to limit the range of auxiliary data connections (a single or range of port numbers) for protocols having control and data connections (like FTP). The trigger port will be the destination port of an association which matches a rule.

- *port_number*: Specifies the auxiliary port number to open for traffic, and must be an integer from 1 through 65535.

- **range** *start_port* **to** *end_port*: Specifies the range of port numbers to open for subscriber traffic.
  - *start_port* must be an integer from 1 through 65535.
  - *end_port* must be an integer from 1 through 65535, and must be greater than *start_port*.
- **direction { both | reverse | same }**: Specifies the direction from which the auxiliary connection is initiated. This direction can be same as the direction of control connection, or the reverse of the control connection direction, or in both directions.
  - *both*: Provides the trigger to open port for traffic in either direction of the control connection.
  - *reverse*: Provides the trigger to open port for traffic in the reverse direction of the control connection (from where the connection is initiated).
  - *same*: Provides the trigger to open port for traffic in the same direction of the control connection (from where the connection is initiated).

Usage

Use this command to add access ruledefs to the Firewall-and-NAT policy and configure the priority and actions for rule matching.
The policy specifies the rules to be applied on calls. The ruledefs in the policy have priorities, based on which priority matching is done.
For Stateful Firewall, the port trigger configuration is optional, and can be configured only if a rule action is permit. When a rule is matched and the rule action is permit, if the trigger is configured, the appropriate check is made. The trigger port will be the destination port of an association that matches the rule. Multiple triggers can be defined for the same port number to permit multiple auxiliary ports for subscriber traffic.
When a rule is matched and if the rule action is deny, the action taken depends on what is configured in the specified charging action. If the flow exists, flow statistics are updated and action is taken as configured in the charging action:

- If the billing action is configured as Event Data Record (EDR) enabled, an EDR is generated.
- If the content ID is configured, UDR information is updated.
- If the flow action is configured as “terminate-flow”, the flow is terminated instead of just discarding the packet.

If the billing action, content ID, and flow action are not configured, no action is taken on the dropped packets.

Important: For Stateful Firewall, only the terminate-flow action is applicable if configured in the specified charging action.

Allowing/dropping of packets is determined in the following sequence:

- Check is done to see if the packet matches any pinholes. If yes, no rule matching is done and the packet is allowed.
- Access ruledef matching is done. If a rule matches, the packet is allowed or dropped as per the **access-rule priority** configuration.
- If no access ruledef matches, the packet is allowed or dropped as per the **access-rule no-ruledef-matches** configuration.

For a packet dropped due to access ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the **access-rule priority** or the **access-rule no-ruledef-matches** command respectively.

For action on packets dropped due to any error condition after data session is created, the charging action must be configured in the **flow any-error charging-action** command in the ACS Rulebase Configuration Mode.
The GGSN can dynamically activate or deactivate dynamic ruledefs for a subscriber based on the rule name received from a policy server. At rule match, if a rule in the policy is a dynamic rule, and if the rule is enabled for the particular subscriber, rule matching is done for the rule. If the rule is disabled for the particular subscriber, rule matching is not done for the rule.

Example

For Stateful Firewall, the following command assigns a priority of *10* to the access ruledef *test_rule*, adds it to the policy, and permits port trigger to be used for the rule to open ports in the range of *1000* to *2000* in either direction of the control connection:

```
access-rule priority 1 access-ruledef test_rule permit trigger open-port
range 1000 to 2000 direction both
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

firewall dos-protection

This command configures Stateful Firewall protection for subscribers from Denial-of-Service (DoS) attacks.

Important: In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] firewall dos-protection { all | flooding { icmp | tcp-syn | udp } | ftp-bounce |
ip-unaligned-timestamp | ipv6-dst-options [ invalid-options | unknown-options ] | ipv6-
extension-hdrs [ limit extension_limit ] | ipv6-frag-hdr nested-fragmentation | ipv6-hop-
by-hop [ invalid-options | jumbo-payload | router-alert | unknown-options ] | mime-flood
| port-scan | source-router | tcp-window-containment | teardrop | winnuke }

default firewall dos-protection
```

no

Disables Stateful Firewall protection for subscribers against the specified Denial of Service (DoS) attack(s).

default

Disables Stateful Firewall protection for subscribers against all DoS attacks.

all

Enables Stateful Firewall protection for subscribers against all DoS attacks supported by the Stateful Firewall service.
The IPv6 extension headers will be enabled only if the **firewall validate-ip-options** command is enabled in the Firewall-and-NAT policy configuration.

flooding { icmp | tcp-syn | udp }

Enables protection against the specified flooding attack:

- **icmp**: Enables protection against ICMP Flood attack.
- **tcp-syn**: Enables protection against TCP Syn Flood attack.
- **udp**: Enables protection against UDP Flood attack.

ftp-bounce

Enables protection against FTP Bounce attacks.

ip-unaligned-timestamp

Enables protection against IP Unaligned Timestamp attacks.

ipv6-dst-options [invalid-options | unknown-options]

Drops IPv6 packets containing the IPv6 destination options header.
The following options are specified in the Destination Options extension header:

- The Tunnel Encapsulation Limit (option type: 0x04) is a destination option defined in RFC 2473.
- The Home Address option (option type: 0xC9) is part of Mobile IP processing defined in RFC 3775. This option is only valid as a Destination Option.
- The NSAP Address option (option type: 0xC3) is assigned as a Destination Option by RFC 1888 and deprecated (reclassified as historic) by RFC 4048.
- **invalid-options**: Drops IPv6 packets containing invalid IPv6 destination options.

  The following values are invalid in a Destination Options extension header option type field. Packets with these options in a Destination Options header will be dropped.

  - Value 0xC2, Jumbo Payload
  - Value 0x05, Router Alert
  - Value 0x06, Quick start
  - Value 0x07, CALIPSO
- **unknown-options**: Drops IPv6 packets containing unknown IPv6 destination options.

ipv6-extension-hdrs [limit *extension_limit* **]**

Default: 8
Limits the number of IPv6 extension headers in an IPv6 packet. An IPv6 packet can contain zero or more extension headers.
Firewall will not fully parse packets with unknown extension headers as the extension header format is unspecified. Under such cases, the transport protocol will be considered as **unknown**. Packets with invalid length field in the extension headers and packets with next header 0x01 (ICMPv4) will be dropped. IPv6 uses ICMPv6 of type 0x3A.
extension_limit must be an integer from 0 through 4294967295.

ipv6-frag-hdr nested-fragmentation

Drops IPv6 packets containing nested fragmentation (reassembled packets containing a fragment header). IPv6 fragmentation is done only by the source node. An IPv6 fragment packet must have only one fragment header. Firewall will drop packets with more than one fragment header. The Reassembled packet containing a fragment header will be dropped by Firewall. As per RFC 2460, the fragment length (except for last fragment) must be a multiple of 8 octets. If not, such fragments are dropped.

ipv6-hop-by-hop [invalid-options | jumbo-payload | router-alert | unknown-options]

Drops IPv6 packets containing the hop-by-hop extension header.
The Hop-by-Hop Options extension header, if present, must be the first header to follow the IPv6 main header. This is indicated by a value of 0x00 in the next header field in the main header. The length must be expressed as a multiple of 8 octets (excluding the first 8 octets). If not, such packets will be dropped.

- **invalid-options**: Drops IPv6 packets containing invalid IPv6 hop-by-hop options.

The following values are invalid in a Hop-by-Hop extension header option type field. Packets with these options in a hop-by-hop header will be dropped.

- Value 0x04, Tunnel Encapsulation limit
- Value 0xC9, Home Address Destination option
- Value 0xC3, NSAP Address option

The options are present in TLV (Type Length Value) format. If the length specified is invalid, then such packets will be dropped.

- **jumbo-payload**: Drops IPv6 packets with jumbo payload hop-by-hop options.

  The Jumbo Payload option (RFC 2675) has the option type value 0xC2 and is only valid as a Hop-by-Hop option. This option allows the creation of very large IP packets (packets larger than 65K bytes). If this option is allowed, the following validity checks will be done.

  - The IP payload length must be 0x00 when the Jumbo Payload option is present.
  - The Jumbo Payload option must be used only when the length is greater than 65,535; the two most significant bytes of the Jumbo length cannot be 0x00.
  - The Jumbo Payload option cannot be used in conjunction with a Fragmentation extension header.

  If any of the above checks fail, then the IPv6 packet will be dropped. The Option Type field must have 4n+2 alignment.

- **router-alert**: Drops IPv6 packets with router alert hop-by-hop options.

  The Router Alert (RFC 2711) option is used to signal the routers that a closer inspection of the packet is warranted. Denial of service (DoS) attacks can occur if an attacker sends large number of packets with this option. Only one option of this type must be present, regardless of value, per Hop-by-Hop header with 2n + 0 alignment.

- **unknown-options**: Drops IPv6 packets containing unknown IPv6 hop-by-hop options.

mime-flood

Enables protection against HTTP Multiple Internet Mail Extension (MIME) header flooding attacks.

port-scan

Enables protection against Port Scan attacks.

tcp-window-containment

Enables protection against TCP sequence number out-of-range attacks.

source-router

Enables protection against IPv4/IPv6 Source Route IP Option attacks.
This command can be used to filter IPv4/IPv6 packets containing Routing header of Type 0 (source routing). In this release, only type 0 filtering is supported.

teardrop

Enables protection against IPv4/IPv6 Teardrop attacks.

winnuke

Enables protection against WIN-NUKE attacks.

Usage

Use this command to enable Stateful Firewall protection from different types of DoS attacks. This command can be used multiple times for different DoS attacks.

Important: DoS attacks are detected only in the downlink direction.

Example

The following command enables protection from all supported DoS attacks:

```
firewall dos-protection all
```

firewall flooding

This command configures Stateful Firewall protection from Packet Flooding attacks.

Important: In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall flooding { protocol { icmp | tcp-syn | udp } packet limit *packets* **| sampling-interval** *interval* **}**

default firewall flooding { protocol { icmp | tcp-syn | udp } packet limit | sampling-interval }

default

Configures the default setting for the specified configuration.

protocol { icmp | tcp-syn | udp }

Specifies the transport protocol:

- **icmp**: Configuration for ICMP protocol.
- **tcp-syn**: Configuration for TCP-SYN packet limit.
- **udp**: Configuration for UDP protocol.

packet limit *packets*

Specifies the maximum number of specified packets a subscriber can receive during a sampling interval.
packets must be an integer from 1 through 4294967295.
Default: 1000 packets per sampling interval for all protocols.

sampling-interval *interval*

Specifies the flooding sampling interval, in seconds.
interval must be an integer from 1 through 60.
Default: 1 second
The maximum sampling-interval configurable is 60 seconds.

Usage

Use this command to configure the maximum number of ICMP, TCP-SYN, / UDP packets allowed to prevent the packet flooding attacks to the host.

Example

The following command ensures a subscriber will not receive more than *1000* ICMP packets per sampling interval:

```
firewall flooding protocol icmp packet limit 1000
```

The following command ensures a subscriber will not receive more than *1000* UDP packets per sampling interval on different 5-tuples. That is, if an attacker is sending lot of UDP packets on different ports or using different spoofed IP addresses, those packets will be limited to 1000 packets per sampling interval. This way only “suspected” malicious packets are limited and not “legitimate” packets.

```
firewall flooding protocol udp packet limit 1000
```

The following command ensures a subscriber will not receive more than *1000* TCP-Syn packets per sampling interval:

```
firewall flooding protocol tcp-syn packet limit 1000
```

The following command specifies a flooding sampling interval of *1* second:

```
firewall flooding sampling-interval 1
```

firewall icmp-checksum-error

This command configures Stateful Firewall action on packets with ICMP/ICMPv6 Checksum errors.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
firewall icmp-checksum-error { drop | permit }

default firewall icmp-checksum-error
```

default

Configures the default setting.
Default: **drop**

drop

Drops packets with ICMP/ICMPv6 Checksum errors.

permit

Permits packets with ICMP/ICMPv6 Checksum errors.

Usage

Use this command to configure Stateful Firewall action on packets with ICMP/ICMPv6 Checksum errors. This command also applies to ICMP/ICMPv6 packets with Inner IP Checksum error.
For NAT-only calls, packets with ICMP/ICMPv6 errors are dropped, and other packets are allowed.

Example

The following command configures Stateful Firewall to drop packets with ICMP/ICMPv6 Checksum errors:

```
firewall icmp-checksum-error drop
```

firewall icmp-destination-unreachable-message-threshold

This command configures a threshold on the number of ICMP/ICMPv6 error messages sent by the subscriber for a particular data flow.

Important: In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
firewall icmp-destination-unreachable-message-threshold messages then-block-server

{ default | no } firewall icmp-destination-unreachable-message-threshold
```

default

Configures the default setting.
Default: No limit

no

Removes the previous configuration.

messages

Specifies the threshold on the number of ICMP/ICMPv6 error messages sent by the subscriber for a particular data flow. *messages* must be an integer from 1 through 100.

Usage

Use this command to configure a threshold on the number of ICMP/ICMPv6 error messages sent by the subscriber for a particular data flow. After the threshold is reached, it is assumed that the server is not reacting properly to the error messages, and further downlink traffic to the subscriber on the unwanted flow is blocked.
Some servers that run QChat ignore the ICMP/ICMPv6 error messages (Destination Port Unreachable and Host Unreachable) from the mobiles. So the mobiles continue to receive unwanted UDP traffic from the QChat servers, and their batteries get exhausted quickly.

Example

The following command configures a threshold of *10* ICMP/ICMPv6 error messages:

```
firewall icmp-destination-unreachable-message-threshold 10 then-block-
server
```

firewall icmp-echo-id-zero

This command configures Stateful Firewall action on echo packets with ICMP/ICMPv6 ID zero.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
firewall icmp-echo-id-zero { drop | permit }

default firewall icmp-echo-id-zero
```

default

Configures the default setting.
Default: **permit**

drop

Drops packets with ICMP/ICMPv6 ID zero.

permit

Permits packets with ICMP/ICMPv6 ID zero.

Usage

Use this command to configure Stateful Firewall action on echo packets with ICMP/ICMPv6 ID zero.

Example

The following command configures Stateful Firewall to drop packets with ICMP/ICMPv6 ID zero:

```
firewall icmp-echo-id-zero drop
```

firewall icmp-fsm

This command enables/disables Stateful Firewall's ICMP/ICMPv6 Finite State Machine (FSM).

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] firewall icmp-fsm
```

default

Configures the default setting.
Default: Enabled. Same as **firewall icmp-fsm**.

no

Disables Stateful Firewall ICMP/ICMPv6 FSM checks.

Usage

Use this command to enable/disable Stateful Firewall ICMP/ICMPv6 FSM checks. When Stateful Firewall and ICMP/ICMPv6 FSM are enabled, ICMP/ICMPv6 reply messages for which there is no saved ICMP/ICMPv6 request message are discarded. ICMP/ICMPv6 error messages (i.e., messages containing an embedded message) for which there is no saved flow for the embedded message are discarded.

Example

The following command disables Stateful Firewall's ICMP/ICMPv6 FSM checks:

```
no firewall icmp-fsm
```

firewall ip-reassembly-failure

This command configures Stateful Firewall action on IPv4/IPv6 packets involved in IP Reassembly Failure scenarios.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
firewall ip-reassembly-failure { drop | permit }

default firewall ip-reassembly-failure
```

default

Configures the default setting.
Default: **permit**

drop

Drops IPv4/IPv6 packets involved in IP reassembly failure scenarios.

permit

Permits IPv4/IPv6 packets involved in IP reassembly failure scenarios.

Usage

Use this command to configure Stateful Firewall action on IPv4/IPv6 packets involved in IP reassembly failure scenarios such as missing fragments, overlapping offset, etc.
For NAT-only calls, packets involved in IP reassembly failure scenarios are dropped.

Example

The following command specifies to drop IPv4/IPv6 packets involved in IP reassembly failure scenarios:

```
firewall ip-reassembly-failure drop
```

firewall malformed-packets

This command configures Stateful Firewall action on malformed packets. In release 12.0, this command supports ICMPv6 and IPv6 packets.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
firewall malformed-packets { drop | permit }

default firewall malformed-packets
```

default

Configures the default setting.
Default: **permit**

drop

Drops malformed packets.

permit

Permits malformed packets.

Usage

Use this command to configure Stateful Firewall action on malformed packets.
For NAT-only calls, malformed packets are always permitted.

Example

The following command specifies Stateful Firewall to drop malformed packets:

```
firewall malformed-packets drop
```

firewall max-ip-packet-size

This command configures the maximum IPv4/IPv6 packet size (after IP reassembly) allowed over Stateful Firewall.

Important: In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall max-ip-packet-size *packet_size* **protocol { icmp | non-icmp }**

default firewall max-ip-packet-size protocol { icmp | non-icmp }

default

Configures the default setting.
Default: 65535 bytes (for both ICMP/ICMPv6 and non-ICMP/ICMPv6)

packet_size

Specifies the maximum packet size allowed by firewall. Any IPv6 packet with payload size greater than the configured value will be dropped.
packet_size must be an integer from 30000 through 65535.

protocol { icmp | non-icmp }

Specifies the transport protocol:

- **icmp**: Configuration for ICMP/ICMPv6 protocol.
- **non-icmp**: Configuration for protocols other than ICMP/ICMPv6.

Usage

Use this command to configure the maximum IPv4/IPv6 packet size allowed for ICMP/ICMPv6 and non-ICMP/ICMPv6 packets to prevent packet flooding attacks to the host. Packets exceeding the configured size will be dropped for “Jolt” and “Ping-Of-Death” attacks.

Example

The following command allows a maximum packet size of *60000* for ICMP/ICMPv6 protocol:

```
firewall max-ip-packet-size 60000 protocol icmp
```

firewall mime-flood

This command configures Stateful Firewall protection from MIME Flood attacks.

Important: In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall mime-flood { http-headers-limit *max_limit* **| max-http-header-field-size** *max_size* **}**

default firewall mime-flood { http-headers-limit | max-http-header-field-size }

default

Configures the default setting for the specified parameter.

http-headers-limit *max_limit*

Specifies the maximum number of headers allowed in an HTTP packet. If the number of HTTP headers in a page received is more than the specified limit, the request will be denied.
max_limit must be an integer from 1 through 256.
Default: 16

max-http-header-field-size *max_size*

Specifies the maximum header field size allowed in the HTTP header, in bytes. If the size of HTTP header in the received page is more than the specified number of bytes, the request will be denied.
max_size must be an integer from 1 through 8192.
Default: 4096 bytes

Usage

Use this command to configure the maximum number of headers allowed in an HTTP packet, and the maximum header field size allowed in the HTTP header to prevent MIME flooding attacks.
This command is only effective if Stateful Firewall DoS protection for MIME flood attacks has been enabled using the **firewall dos-protection mime-flood** command, and the **route** command has been configured to send HTTP packets to the HTTP analyzer.

Example

The following command sets the maximum number of headers allowed in an HTTP packet to *100*:

```
firewall mime-flood http-headers-limit 100
```

The following command sets the maximum header field size allowed in the HTTP header to *1000* bytes:

```
firewall mime-flood max-http-header-field-size 1000
```

firewall policy

This command enables/disables Stateful Firewall support in a Firewall-and-NAT policy.

Important: In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

In 11.0 and earlier releases:

```
firewall policy firewall-required
```

```
no firewall policy
```

In 12.0 and later releases:

```
firewall policy { ipv4-and-ipv6 | ipv4-only | ipv6-only }
```

```
{ default | no } firewall policy
```

default

Disables IPv4 and IPv6 Stateful Firewall support in the Firewall-and-NAT policy.

no

Disables IPv4 and IPv6 Stateful Firewall support in the Firewall-and-NAT policy.

firewall-required

Enables Stateful Firewall support in the Firewall-and-NAT policy.

Important: This keyword is available only in 11.0 and earlier releases.

ipv4-and-ipv6

Enables both IPv4 and IPv6 Stateful Firewall support in the Firewall-and-NAT policy.

ipv4-only

Enables IPv4 Stateful Firewall and disables IPv6 Stateful Firewall in the Firewall-and-NAT policy.

ipv6-only

Enables IPv6 Stateful Firewall and disables IPv4 Stateful Firewall support in the Firewall-and-NAT policy.

Usage

Use this command to enable/disable IPv4 and/or IPv6 Stateful Firewall support for all subscribers using a Firewall-and-NAT policy.

Example

The following command enables IPv4 and IPv6 Stateful Firewall support in a Firewall-and-NAT policy:

```
firewall policy ipv4-and-ipv6
```

The following command disables Stateful Firewall support in a Firewall-and-NAT policy:

```
no firewall policy
```

firewall tcp-checksum-error

This command configures Stateful Firewall action on packets with TCP Checksum error.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
firewall tcp-checksum-error { drop | permit }

default firewall tcp-checksum-error
```

default

Configures the default setting.
Default: **drop**

drop

Drops packets with TCP Checksum errors.

permit

Permits packets with TCP Checksum errors.

Usage

Use this command to configure Stateful Firewall action on packets with TCP Checksum error.
For NAT-only calls, packets with TCP Checksum errors are permitted.

Example

The following command specifies Stateful Firewall to drop packets with TCP Checksum errors:

```
firewall tcp-checksum-error drop
```

firewall tcp-first-packet-non-syn

This command configures Stateful Firewall action on TCP flows starting with a non-SYN packet.

Important: In release 9.0, this command is deprecated. This configuration is available as the **`firewall tcp-fsm [ first-packet-non-syn { drop | permit | send-reset } ]`** command.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

`firewall tcp-first-packet-non-syn { drop | reset }`

`default firewall tcp-first-packet-non-syn`

`default`

Configures the default setting.
Default: **`drop`**

`drop`

Drops the non-SYN packet.

`reset`

Sends reset.

Usage

Use this command to configure Stateful Firewall action on TCP flows starting with a non-SYN packet.

Example

For flows starting with a non-SYN packet, the following command specifies Stateful Firewall to drop the non-SYN packet:

```
firewall tcp-first-packet-non-syn drop
```

firewall tcp-fsm

This command enables/disables Stateful Firewall's TCP Finite State Machine (FSM).

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall tcp-fsm [first-packet-non-syn { drop | permit | send-reset }]

{ default | no } firewall tcp-fsm

default

Configures the default setting.
Default: **drop**

no

Disables Stateful Firewall's TCP FSM.

first-packet-non-syn { drop | permit | send-reset }

Specifies Stateful Firewall action on TCP flows starting with a non-SYN packet:

- **drop**: Specifies to drop the packet.
- **permit**: Specifies to permit the packet.
- **send-reset**: Specifies to drop the packet and send TCP RST.

Default: **drop**

Usage

Use this command to enable/disable Stateful Firewall's TCP FSM checks. When Stateful Firewall and TCP FSM are enabled, state of the TCP session is checked to decide whether to forward TCP packets.

Example

The following command enables TCP FSM, and configures action to take on TCP flows starting with a non-SYN packet to drop the packet:

```
firewall tcp-fsm first-packet-non-syn drop
```

firewall tcp-idle-timeout-action

This command configures action on TCP idle timeout expiry.

Important: In release 9.0 and later this command is also available to NAT.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

```
firewall tcp-idle-timeout-action { drop | reset }

{ default | no } firewall tcp-idle-timeout-action
```

default

Configures the default setting.
Default: **reset**

no

Configures the TCP idle timeout expiry action to reset.

drop

Drops the session on TCP idle timeout expiry.

reset

Resends TCP RST on TCP idle timeout expiry. When configured to reset, the session is dropped, and the system can avoid packets arriving for the idle flow from getting dropped.

Usage

Use this command to configure action to take on TCP idle timeout expiry.

Example

The following command configures action to take on TCP idle timeout expiry to drop:

```
firewall tcp-idle-timeout-action drop
```

firewall tcp-options-error

This command configures Stateful Firewall action on packets with TCP Option errors.

Product

FW

Privileges

Security Administrator, Administrator

Syntax

```
firewall tcp-options-error { drop | permit }

default firewall tcp-options-error
```

default

Configures the default setting.
Default: **permit**

drop

Drops packets with TCP Option errors.

permit

Permits packets with TCP Option errors.

Usage

Use this command to configure Stateful Firewall action on packets with TCP Option errors.

Example

The following command configures Stateful Firewall to drop packets with TCP Option errors:

```
firewall tcp-options-error drop
```

firewall tcp-partial-connection-timeout

This command configures action on idle timeout for partially open TCP connections.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall tcp-partial-connection-timeout *timeout*

{ default | no } firewall tcp-partial-connection-timeout

default

Configures the default setting.

no

Disables the idle timeout for partially open TCP connections.

timeout

Specifies the timeout in seconds.
timeout must be an integer from 0 through 86400.
Default: 30 seconds

Usage

Use this command to configure idle timeout for TCP connections that are yet to be established (partially open) in the case of Firewall enabled calls.

Example

The following command sets the idle timeout setting to *30* seconds:

```
firewall tcp-partial-connection-timeout 30
```

firewall tcp-reset-message-threshold

This command configures a threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. After this threshold is reached, further downlink traffic to the subscriber on the unwanted flow is blocked.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall tcp-reset-message-threshold *messages* **then-block-server**

{ default | no } firewall tcp-reset-message-threshold

default

Configures the default setting.
Default: Disabled

no

Disables the configuration.

messages

Specifies the threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. *messages* must be an integer from 1 through 100.

Usage

Use this command to configure a threshold on the number of TCP reset messages (TCP RST+ACK) sent by the subscriber for a particular data flow. After the threshold is reached, assuming the server is not reacting properly to the reset messages further downlink traffic to the subscriber on the unwanted flow is blocked. This configuration enables QCHAT noise suppression for TCP.

Example

The following command sets the threshold on the number of TCP reset messages to *10*:

```
firewall tcp-reset-message-threshold 10 then-block-server
```

firewall tcp-syn-flood-intercept

This command configures TCP SYN intercept parameters for protection against TCP SYN flooding attacks.

Important: In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

firewall tcp-syn-flood-intercept { mode { none | watch [aggressive] } | watch-timeout *intercept_watch_timeout* **}**

default firewall tcp-syn-flood-intercept { mode | watch-timeout }

default

Configures the default settings for SYN Flood DoS protection.

mode { none | watch [aggressive] }

Specifies the TCP SYN flood intercept mode:

- **none**: Disables the TCP SYN Flood Intercept feature.
- **watch**: Configures TCP SYN flood intercept feature in watch mode. The Stateful Firewall passively watches to see if TCP connections become established within a configurable interval. If connections are not established within the timeout period, the Stateful Firewall clears the half-open connections by sending RST to TCP client and server. The default watch-timeout for connection establishment is 30 seconds.
- **aggressive**: Configures TCP SYN flood Intercept or Watch feature for aggressive behavior. Each new connection request causes the oldest incomplete connection to be deleted. When operating in watch mode, the watch timeout is reduced by half. If the watch-timeout is 30 seconds, under aggressive conditions it becomes 15 seconds. When operating in intercept mode, the retransmit timeout is reduced by half (i.e. if the timeout is 60 seconds, it is reduced to 30 seconds). Thus the amount of time waiting for connections to be established is reduced by half (i.e. it is reduced to 150 seconds from 300 seconds under aggressive conditions).

Default: **none**

watch-timeout *intercept_watch_timeout*

Specifies the TCP intercept watch timeout, in seconds.
intercept_watch_timeout must be an integer from 5 through 30.
Default: 30

Usage

This TCP intercept functionality provides protection against TCP SYN Flooding attacks. This command enables and configures TCP intercept parameters to prevent TCP SYN flooding attacks by intercepting and validating TCP connection requests for DoS protection mechanism configured with the **dos-protection** command.

The system captures TCP SYN requests and responds with TCP SYN-ACKs. If a connection initiator completes the handshake with a TCP ACK, the TCP connection request is considered as valid by system and system forwards the initial TCP SYN to the valid target which triggers the target to send a TCP SYN-ACK. Now system intercepts with TCP SYN-ACK and sends the TCP ACK to complete the TCP handshake. Any TCP packet received before the handshake completion will be discarded.

Example

The following command sets the intercept watch timeout setting to *15* seconds:

```
firewall tcp-syn-flood-intercept watch-timeout 15
```

firewall tcp-syn-with-ecn-cwr

This command configures Stateful Firewall action on TCP SYN packets with either ECN or CWR flag set.

Product

FW

Privileges

Security Administrator, Administrator

Syntax

```
firewall tcp-syn-with-ecn-cwr { drop | permit }

default firewall tcp-syn-with-ecn-cwr
```

default

Configures the default setting.
Default: **permit**

drop

Drops TCP SYN packets with either ECN or CWR flag set.

permit

Permits TCP SYN packets with either ECN or CWR flag set.

Usage

Use this command to configure Stateful Firewall action on receiving a TCP SYN packet with either ECN or CWR flag set.

Example

The following command configures Stateful Firewall to drop TCP SYN packets with ECN / CWR flag set:

```
firewall tcp-syn-with-ecn-cwr drop
```

firewall udp-checksum-error

This command configures Stateful Firewall action on packets with UDP Checksum error.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
firewall udp-checksum-error { drop | permit }

default firewall udp-checksum-error
```

default

Configures the default setting.
Default: **drop**

drop

Drops packets with UDP Checksum error.

permit

Permits packets with UDP Checksum error.

Usage

Use this command to configure Stateful Firewall action on packets with UDP Checksum error.
For NAT-only calls, packets with UDP Checksum error are permitted.

Example

The following command specifies to drop packets with UDP Checksum error:

```
firewall udp-checksum-error drop
```

firewall validate-ip-options

This command enables / disables the Stateful Firewall validation of IP options for errors.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] firewall validate-ip-options
```

default

Configures the default setting.
Default: Disabled. Same as **no firewall validate-ip-options**

no

Disables validation of IP options.

Usage

Use this command to enable / disable Stateful Firewall validation of IP options. When enabled, Stateful Firewall will drop packets with IP option errors.
For NAT calls, validation of IP Options is disabled.

Example

The following command enables validation of IP options:

```
firewall validate-ip-options
```

nat binding-record

This command configures the generation of NAT Binding Records.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

nat binding-record edr-format *edr_format* **[port-chunk-allocation] [port-chunk-release]**

{ default | no } nat binding-record

default

Configures the default setting.
Default: **port-chunk-release**

no

Disables generating NAT Binding Records.

edr-format *edr_format*

Specifies the Event Data Record (EDR) format name.
edr_format must be an alphanumeric string of 1 through 63 characters.

port-chunk-allocation

Specifies generating NAT Binding Records when a port-chunk is allocated.

port-chunk-release

Specifies generating NAT Binding Record when a port-chunk is released.

Usage

Use this command to configure the generation of NAT Binding Records.

Example

The following command configures an EDR format named *test123* and specifies generating NAT Binding Records when a port chunk is allocated:

```
nat binding-record edr-format test123 port-chunk-allocation
```

nat icsr-flow-recovery

This command enables/disables the NAT ICSR Flow checkpointing support for subscribers in a Firewall-and-NAT policy.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

```
{ default | no } nat icsr-flow-recovery
```

default

Configures the default setting.
Default: Disabled. Same as **no nat icsr-flow-recovery**.

no

Disables the NAT ICSR Flow checkpointing.

Usage

Use this command to enable/disable all NAT ICSR Flow checkpointing for subscribers using this policy.

Example

The following command enables NAT ICSR Flow checkpointing:

```
nat icsr-flow-recovery
```

nat policy

This command enables/disables Network Address Translation (NAT) support in a Firewall-and-NAT policy.

Important: In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

In 12.1 and earlier releases:

nat policy nat-required [default-nat-realm *nat_realm_name* **[fw-and-nat-action** *action_name* **]]**

no nat policy

In 12.2 and later releases:

nat policy [ipv4-and-ipv6 | ipv4-only | ipv6-only] [default-nat-realm *nat_realm_name* **[fw-and-nat-action** *action_name* **]]**

no nat policy

no

Disables both NAT44 and NAT64 support in the Firewall-and-NAT policy.

nat-required

Enables NAT support in the Firewall-and-NAT policy.

Important: This keyword is available only in 12.1 and earlier releases, and is supported in release 12.2 for backward compatibility. The **nat policy nat-required** command enables only NAT44.

ipv4-and-ipv6

Enables NAT processing for both IPv4 and IPv6 in the Firewall-and-NAT policy.

ipv4-only

Enables NAT processing for IPv4 in the Firewall-and-NAT policy.

ipv6-only

Enables NAT processing for IPv6 in the Firewall-and-NAT policy.

default-nat-realm *nat_realm_name*

Specifies the default NAT realm for the Firewall-and-NAT policy.

nat_realm_name must be the name of an existing NAT realm, and must be an alphanumeric string of 1 through 31 characters.

fw-and-nat-action *action_name*

Specifies the Firewall-and-NAT action name.
action_name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to enable/disable IPv4 and/or IPv6 NAT support for all subscribers using a Firewall-and-NAT policy.
In release 8.1, to enable NAT support for a subscriber, Stateful Firewall must also be enabled for that subscriber. See the **firewall policy** CLI command.
Once NAT is enabled for a subscriber, the NAT IP address to be used is chosen from the NAT realms specified in the rules. See the **access-rule** CLI command.
You can enable/disable NAT at any time, however the changed NAT status will not be applied to active calls. The new NAT status will only be applied to new calls.

Example

The following command enables NAT support in a Firewall-and-NAT policy:

```
nat policy nat-required
```

The following command disables NAT support in a Firewall-and-NAT policy:

```
no nat policy
```

The following command enables IPv4 and IPv6 NAT support in a Firewall-and-NAT policy:

```
nat policy ipv4-and-ipv6
```

nat private-ip-flow-timeout

This command configures the Private IP NPU flow timeout setting.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

```
nat private-ip-flow-timeout timeout

{ default | no } nat private-ip-flow-timeout
```

default

Configures the default setting.
Default: 180 seconds

no

Disables the Private IP NPU flow timeout configuration.
When disabled, the flow is installed at call setup and will be removed only when the subscriber disconnects.

timeout

Specifies the Private IP NPU flow timeout period in seconds.
timeout must be an integer from 180 through 86400.

Usage

Use this command to configure the Private IP NPU flow timeout setting.
For NAT-enabled calls, by default, the downlink private IP NPU flow will not be installed at call setup for a subscriber session. The flow will only be installed on demand. When there is no traffic on the private flow, the private IP flow will be removed after the configurable timeout period.

Example

The following command configures the Private IP NPU flow timeout setting to *36000* seconds:

```
nat private-ip-flow-timeout 36000
```

nat suppress-aaa-update

This command suppresses sending NAT Bind Update (NBU) to the AAA server when PPP disconnect happens.

Important: This command is customer-specific. For more information please contact your local service representative.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

```
nat suppress-aaa-update call-termination

default nat suppress-aaa-update
```

default

Configures the default setting.
Default: No suppression of AAA updates.

Usage

Use this command to suppress sending of NBU to the AAA server when PPP disconnect happens, as these NBUs would be cleared at the AAA after receiving the accounting-stop. This enables to minimize the number of messages between the chassis and AAA server. When not configured, NBU are sent to the AAA server whenever a port chunk is allocated, de-allocated, or the call is cleared (PPP disconnect).

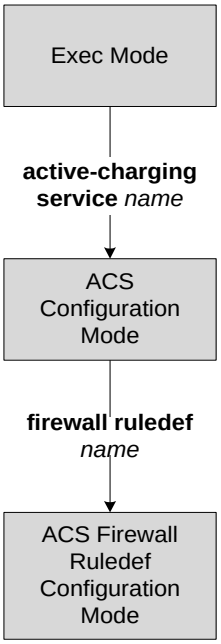
Example

The following command suppresses the sending of NBU to the AAA server:

```
nat suppress-aaa-update call-termination
```

Chapter 123
Firewall-and-NAT Access Ruledef Configuration Mode Commands

The Firewall-and-NAT Access Ruledef Configuration Mode is used to configure and manage Access rule definitions used by the Stateful Firewall (FW) and Network Address Translation (NAT) in-line services.



bearer 3gpp apn

This command configures an access ruledef to analyze user traffic based on APN bearer.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] bearer 3gpp apn [case-sensitive] *operator value*

no

Removes previously configured bearer ruledef.

case-sensitive

This keyword makes the rule case sensitive.
By default, ruledefs are not case sensitive.
Default: Disabled

operator

Specifies how to logically match the APN name.
operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

value

The APN name to match in bearer flow.
value must be an alphanumeric string of 1 through 63 characters that can include punctuation characters.

Usage

Use this command to specify an access ruledef to analyze user traffic based on APN name.

Example

The following command creates an access ruledef for analyzing user traffic for an APN named *apn12*:

```
bearer 3gpp apn = apn12
```

bearer 3gpp imsi

This command configures an access ruledef to analyze user traffic based on International Mobile Station Identification (IMSI) number in bearer flow.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] bearer 3gpp imsi { *operator msid* **| { !range | range } imsi-pool** *imsi_pool* **}**

---

no

Removes previously configured bearer ruledef.

---

operator

Specifies how to logically match the MSID.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

---

msid

Specifies the Mobile Station Identifier.

{ !range | range } imsi-pool *imsi_pool*

{ !range | range }: Specifies the range criteria:

- **!range**: Not in the range of
- **range**: In the range of

imsi-pool *imsi_pool*: Specifies the IMSI pool name. *imsi_pool* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify an access ruledef to analyze user traffic based on IMSI number of mobile station.

Example

The following command creates an access ruledef to analyze user traffic for the IMSI number *9198838330912*:

```
bearer 3gpp imsi = 9198838330912
```

bearer username

This command configures an access ruledef to analyze user traffic based on user name of the bearer flow.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

`[ no ] bearer username [ case-sensitive ]` *`operator value`*

`no`

Removes previously configured bearer ruledef.

`case-sensitive`

This keyword makes the rule case sensitive.
By default, ruledefs are not case sensitive.
Default: Disabled

`operator`

Specifies how to logically match the MSID.
`operator` must be one of the following:

- **`!=`**: Does not equal
- **`!contains`**: Does not contain
- **`!ends-with`**: Does not end with
- **`!starts-with`**: Does not start with
- **`=`**: Equals
- **`contains`**: Contains
- **`ends-with`**: Ends with
- **`starts-with`**: Starts with

`value`

Specifies the user name.
`value` must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to specify a access ruledef to analyze user traffic based on user name of the bearer flow.

Example

The following command creates an access ruledef for analyzing user traffic for the user name *`user12`*:

```
bearer username = user12
```

create-log-record

This command enables/disables access ruledef logging.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] create-log-record
```

no

Disables access ruledef logging.

Usage

Use this command to enable/disable access ruledef logging.

Example

The following command enables access ruledef logging:

```
create-log-record
```

The following command disables access ruledef logging:

```
no create-log-record
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

icmp any-match

This command configures an access ruledef to match any ICMPv4 traffic for the user.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] icmp any-match *operator condition*

no

Removes previously configured ICMPv4 any-match ruledef.

operator

Specifies how to logically match the analyzed state.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to be matched for the user traffic.
condition must be one of the following:

- **FALSE**: Specified condition is FALSE.
- **TRUE**: Specified condition is TRUE.

Usage

Use this command to specify an access ruledef to match any ICMPv4 traffic of the user.

Example

The following command creates an access ruledef to match any non-ICMPv4 traffic of the user:

```
icmp any-match = FALSE
```

icmp code

This command configures an access ruledef to analyze user traffic based on ICMPv4 code.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] icmp code *operator code*

no

Removes previously configured ICMPv4 code ruledef.

operator

Specifies how to logically match the ICMPv4 code.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

code

Specifies the ICMPv4 code.
code must be an integer from 0 through 255.

Usage

Use this command to define an access ruledef to analyze user traffic based on the ICMPv4 code.

Example

The following command creates an access ruledef for analyzing user traffic using the ICMPv4 code as *23*:

```
icmp code = 23
```

icmp type

This command configures an access ruledef to analyze user traffic based on ICMPv4 type.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] icmp type operator type
```

no

Removes previously configured ICMPv4 type ruledef.

operator

Specifies how to logically match the ICMPv4 type.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

type

Specifies the ICMPv4 type.
type must be an integer from 0 through 255.
For example, 0 for ECHO Reply, 3 for Dest. Unreachable, and 5 for Redirect.

Usage

Use this command to define an access ruledef to analyze user traffic based on the ICMPv4 type.

Example

The following command creates an access ruledef for analyzing user traffic using an ICMPv4 type as *123*:

```
icmp type = 123
```

icmpv6 any-match

This command configures an access ruledef to match any ICMPv6 traffic for the user.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] icmpv6 any-match *operator condition*

no

Removes previously configured ICMPv6 any-match ruledef.

operator

Specifies how to logically match the analyzed state.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to be matched for the user traffic.
condition must be one of the following:

- **FALSE**: Specified condition is FALSE.
- **TRUE**: Specified condition is TRUE.

Usage

Use this command to specify an access ruledef to match any ICMPv6 traffic of the user.

Example

The following command creates an access ruledef to match any non-ICMPv6 traffic of the user:

```
icmpv6 any-match = FALSE
```

icmpv6 code

This command configures an access ruledef to analyze user traffic based on ICMPv6 code.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] icmpv6 code *operator code*

no

Removes previously configured ICMPv6 code ruledef.

operator

Specifies how to logically match the ICMPv6 code.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

code

Specifies the ICMPv6 code.
code must be an integer from 0 through 255.

Usage

Use this command to define an access ruledef to analyze user traffic based on the ICMPv6 code.

Example

The following command creates an access ruledef for analyzing user traffic using the ICMPv6 code as *23*:

```
icmpv6 code = 23
```

icmpv6 type

This command configures an access ruledef to analyze user traffic based on ICMPv6 type.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] icmpv6 type *operator type*

no

Removes previously configured ICMPv6 type ruledef.

operator

Specifies how to logically match the ICMPv6 type.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

type

Specifies the ICMPv6 type.
type must be an integer from 0 through 255.
For example, 0 for ECHO Reply, 3 for Dest. Unreachable, and 5 for Redirect.

Usage

Use this command to define an access ruledef to analyze user traffic based on the ICMPv6 type.

Example

The following command creates an access ruledef for analyzing user traffic using an ICMPv6 type as *123*:

```
icmpv6 type = 123
```

ip any-match

This command configures an access ruledef to match any IP traffic for the user.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] ip any-match *operator condition*

no

Removes previously configured IP any-match ruledef.

operator

Specifies how to logically match the analyzed state.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to be matched for the user traffic.
condition must be one of the following:

- **FALSE**: Specified condition is FALSE.
- **TRUE**: Specified condition is TRUE.

Usage

Use this command to specify an access ruledef to match any IP traffic of the user.

Example

The following command creates an access ruledef to match any non-IP traffic of the user:

```
ip any-match = FALSE
```

ip downlink

This command configures an access ruledef to analyze user traffic based on IP packet flow in downlink direction (to subscriber).

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] ip downlink *operator condition*

no

Removes previously configured IP ruledef.

operator

Specifies how to logically match the packet flow direction.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **TRUE**: Analyzed
- **FALSE**: Not analyzed

Usage

Use this command to define an access ruledef to analyze user traffic based on the IP packet flow direction as downlink.

Example

The following command creates access ruledef for analyzing user traffic using an IP packet direction to downlink (to subscriber):

```
ip downlink = TRUE
```

ip dst-address

This command configures an access ruledef to analyze user traffic based on IP destination address.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ip dst-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask } | {
!range | range } host-pool host_pool }
```

no

Removes previously configured IP destination address ruledef.

operator **{** *ipv4/ipv6_address* **|** *ipv4/ipv6_address/mask* **}**

operator specifies how to logically match the IP destination address.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

ipv4/ipv6_address: Specifies the IP address of destination node for outgoing traffic.
ipv4/ipv6_address must be the IP address entered using dotted-decimal notation for IPv4 or colon-separated notation for IPv6.
ipv4/ipv6_address/mask: Specifies the IP address of destination node for outgoing traffic.
ipv4/ipv6_address/mask must be the IP address entered using dotted-decimal notation for IPv4 or colon-separated notation for IPv6. The mask bit is a numeric value which is the number of bits in the subnet mask.

{ !range | range } host-pool *host_pool* **}**

!range | range: Specifies the range criteria:

- **!range**: Not in the range of
- **range**: In the range of

host-pool *host_pool*: Specifies the host pool name. *host_pool* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify an access ruledef to analyze user traffic based on the IP destination address.

Example

The following command creates IP ruledef for analyzing user traffic using an IP destination address of *10.1.1.1*:

```
ip dst-address = 10.1.1.1
```

ip protocol

This command configures an access ruledef to analyze user traffic based on the protocol being transported by IP packets.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] ip protocol { { *operator* { *protocol* | *protocol_assignment* } } | { *operator protocol_assignment* } }

---

no

Removes previously configured IP protocol address ruledef.

---

operator **{** *protocol* **|** *protocol_assignment* **}**

operator: Specifies how to logically match the IP protocol.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

protocol: Specifies the protocol by name.
protocol must be one of the following:

- ah
- esp
- gre
- icmp
- tcp
- udp

protocol_assignment: Specifies the protocol by assignment number. *protocol_assignment* must be an integer from 0 through 255 (for example, 1 for ICMP, 6 for TCP, and 17 for UDP).

---

operator protocol_assignment

operator: Specifies how to logically match the IP protocol.
operator must be one of the following:

- **<=**: Less than or equals
- **>=**: Greater than or equals

protocol_assignment: Specifies the protocol by assignment number.
protocol_assignment must be an integer from 0 through 255 (for example, 1 for ICMP, 6 for TCP, and 17 for UDP).

Usage

Use this command to specify an access ruledef to analyze user traffic based on the IP protocol.

Example

The following command creates IP ruledef for analyzing user traffic using a protocol assignment of *1*:

```
ip protocol = 1
```

ip server-ipv6-network-prefix

This command configures an access ruledef to analyze user traffic based on IPv6 server prefix.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] ip server-ipv6-network-prefix *operator ipv6_prefix/prefix_length*

no

Removes previously configured IPv6 server prefix.

operator ipv6_prefix/prefix_length

operator: Specifies how to logically match the IPv6 server prefix.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

ipv6_prefix/prefix_length: Specifies the server's IPv6 address with subnet mask bit.
ipv6_prefix/prefix_length must be an IPv6 address in colon-separated notation with subnet mask bit. The *prefix_length* is the number of bits to match. The configurable prefix length values are 32, 40, 48, 56, 64 and 96.

Usage

Use this command to specify an access ruledef to analyze user traffic based on IPv6 server prefix. When a first packet for a flow is received, it is matched against a set of rules configured in the Firewall-and-NAT policy. If the incoming IPv6 packet matches a ruledef and configured prefix, then it indicates that NAT64 needs to be applied on the packet. If the packet did not match the prefix configured, then NAT64 will not be applied on the packet. If there is no rule matching the packet or if there is no rule configured, then the incoming IPv6 packet is matched against the well-known prefix. If the well-known prefix matches, then NAT64 is applied on the packet.

Example

The following command creates an IP ruledef to analyze user traffic using the IPv6 server prefix *abcd:dcba* with *32* bits of the server IPv6 address:

```
ip server-ipv6-network-prefix = abcd:dcba::/32
```

ip src-address

This command configures an access ruledef to analyze user traffic based on IP source address.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ip src-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask } | {
!range | range } host-pool host_pool }
```

no

Removes previously configured IP destination address ruledef.

operator **{** *ipv4/ipv6_address* **|** *ipv4/ipv6_address/mask* **}**

operator: Specifies how to logically match the IP source address.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

ipv4/ipv6_address: Specifies the IP address using dotted-decimal notation for IPv4 or colon-separated notation for IPv6.
ipv4/ipv6_address/mask: Specifies the IP address using dotted-decimal notation for IPv4 or colon-separated notation for IPv6 with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.

{ !range | range } host-pool *host_pool*

!range | range: Specifies the range criteria:

- **!range**: Not in the range of
- **range**: In the range of

host-pool *host_pool*: Specifies the host pool name. *host_pool* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify an access ruledef to analyze user traffic based on the IP source address.

Example

The following command creates IP ruledef for analyzing user traffic using an IP source address of *10.1.1.1*:

```
ip src-address = 10.1.1.1
```

ip uplink

This command configures an access ruledef to analyze user traffic based on IP packet flow in the uplink direction (from subscriber).

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] ip uplink *operator condition*

no

Removes previously configured IP uplink match ruledef.

operator

Specifies how to logically match the IP packet flow direction.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.
condition must be one of the following:

- **TRUE**: Not analyzed
- **FALSE**: Analyzed

Usage

Use this command to define an access ruledef to analyze user traffic based on the IP packet flow direction as uplink.

Example

The following command creates access ruledef for analyzing user traffic using an IP packet direction to uplink (from subscriber):

```
ip uplink = TRUE
```

ip version

This command defines rule expressions to match version number in IP header.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ip version = { ipv4 | ipv6 }
```

no

Deletes the specified rule expression.

ipv4

Specifies the rule expression for IP version 4.

ipv6

Specifies the rule expression for IP version 6.

Usage

Use this command to define rule expressions to match IPv4/IPv6 version number in IP header.

Example

The following command defines a rule expression to match user traffic for the IP version **ipv6**:

```
ip version = ipv6
```

tcp any-match

This command configures an access ruledef to match any TCP traffic for the user.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] tcp any-match *operator condition*

no

Removes previously configured TCP any-match ruledef.

operator

Specifies how to logically match the analyzed state.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to be matched for the user traffic.
condition must be one of the following:

- **FALSE**: Specified condition is FALSE.
- **TRUE**: Specified condition is TRUE.

Usage

Use this command to specify an access ruledef to match any TCP traffic of the user.

Example

The following command creates an access ruledef to match any non-TCP traffic of the user:

```
tcp any-match = FALSE
```

tcp dst-port

This command configures an access ruledef to analyze user traffic based on destination TCP port.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] tcp dst-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

---

no

Removes the previously configured destination TCP port ruledef.

---

operator

Specifies how to logically match the port number.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

---

port_number

Specifies the port number to match.
port_number must be an integer from 1 through 65535.

---

range | !range

Specifies the range criteria:

- **!range**: Not in the range
- **range**: In the range

---

start_range **to** *end_range*

Specifies the starting and ending port numbers for the range of destination TCP ports.
start_range must be an integer from 1 through 65535.
end_range must be an integer from 1 through 65535 that is greater than *start_range*.

---

port-map *port_map*

Specifies name of the port-map for the port range.
port_map must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify an access ruledef to analyze user traffic based on destination TCP port.

Example

The following command creates an access ruledef for analyzing user traffic matching destination port for TCP as *10*:

```
tcp dst-port = 10
```

tcp either-port

This command configures an access ruledef to analyze user traffic based on either (destination or source) TCP ports.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] tcp either-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

---

no

Removes previously configured TCP either-port (destination or source) ruledef.

---

operator

Specifies how to logically match the port number.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

---

port_number

Specifies the port number to match.
port_number must be an integer from 1 through 65535.

---

range | !range

Specifies the range criteria:

- **!range**: Not in the range
- **range**: In the range

---

start_range **to** *end_range*

Specifies the starting and ending port numbers for the port range.
start_range must be an integer from 1 through 65535.
end_range must be an integer from 1 through 65535 that is greater than *start_range*.

---

port-map *port_map*

Specifies name of the port-map for the port range.
port_map must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify an access ruledef to analyze user traffic based on either TCP port.

Example

The following command creates an access ruledef for analyzing user traffic matching destination or source port for TCP as *10*:

```
tcp either-port = 10
```

tcp src-port

This command configures an access ruledef to analyze user traffic based on source TCP port.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] tcp src-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

no

Removes previously configured source TCP port ruledef.

operator

Specifies how to logically match the port number.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

port_number

Specifies the port number to match.
port_number must be an integer from 1 to 65535.

range | !range

Specifies the range criteria:

- **!range**: Not in the range
- **range**: In the range

start_range **to** *end_range*

Specifies the starting and ending port numbers for the port range.
start_range must be an integer from 1 through 65535.
end_range must be an integer from 1 through 65535 that is greater than *start_range*.

port-map *port_map*

Specifies name of the port-map for the port range.
port_map must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify an access ruledef to analyze user traffic based on source TCP port.

Example

The following command creates an access ruledef for analyzing user traffic matching source port for TCP as *10*:

```
tcp src-port = 10
```

udp any-match

This command configures an access ruledef to match any UDP traffic for the user.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] udp any-match *operator condition*

no

Removes previously configured UDP any-match ruledef.

operator

Specifies how to logically match the analyzed state.
operator must be one of the following:

- **!=**: does not equal
- **=**: equals

condition

Specifies the condition to be matched for the user traffic.
condition must be one of the following:

- **FALSE**: Specified condition is FALSE.
- **TRUE**: Specified condition is TRUE.

Usage

Use this command to specify an access ruledef to match any UDP traffic of the user.

Example

The following command creates an access ruledef to match any UDP traffic of the user:

```
udp any-match = TRUE
```

udp dst-port

This command configures an access ruledef to analyze user traffic based on destination UDP port.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] udp dst-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

no

Removes previously configured destination UDP ports ruledef.

operator

Specifies how to logically match the port number.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

port_number

Specifies the port number to match.
port_number must be an integer from 1 through 65535.

!range | range

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

start_range **to** *end_range*

Specifies the starting and ending port numbers for the port range.
start_range must be an integer from 1 through 65535.
end_range must be an integer from 1 through 65535 that is greater than *start_range*.

port-map *port_map*

Specifies name of the port-map for the port range.
port_map must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify an access ruledef to analyze user traffic based on destination UDP port.

Example

The following command creates an access ruledef for analyzing user traffic matching destination port for UDP as *10*:

```
udp dst-port = 10
```

udp either-port

This command configures an access ruledef to analyze user traffic based on either (destination or source) UDP port.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] udp either-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

no

Removes previously configured either-port (destination or source) UDP ruledef.

operator

Specifies how to logically match the port number.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

port_number

Specifies the port number to match.
port_number must be an integer from 1 through 65535.

!range | range

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

start_range **to** *end_range*

Specifies the starting and ending port numbers for the port range.
start_range must be an integer from 1 through 65535.
end_range must be an integer from 1 through 65535 that is greater than *start_range*.

port-map *port_map*

Specifies name of the port-map for the port range.
port_map must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify an access ruledef to analyze user traffic based on either UDP port.

Example

The following command creates an access ruledef for analyzing user traffic matching destination or source port for UDP as *10*:

```
udp either-port = 10
```

udp src-port

This command configures an access ruledef to analyze user traffic based on source UDP port.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

[no] udp src-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

no

Removes previously configured source UDP port ruledef.

operator

Specifies how to logically match the port number.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

port_number

Specifies the port number to match.
port_number must be an integer from 1 through 65535.

!range | range

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

start_range **to** *end_range*

Specifies the starting and ending port numbers for the port range.
start_range must be an integer from 1 through 65535.
end_range must be an integer from 1 through 65535 that is greater than *start_range*.

port-map *port_map*

Specifies name of the port-map for the port range.
port_map must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify an access ruledef to analyze user traffic based on source UDP port.

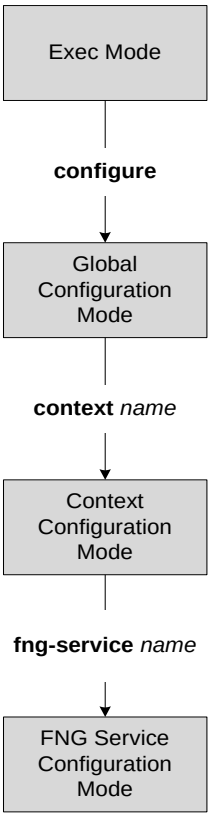
Example

The following command creates an access ruledef for analyzing user traffic matching source port for UDP as *10*:

```
udp src-port = 10
```

Chapter 124
FNG Service Configuration Mode Commands

The FNG Service Configuration Mode is used to configure the properties required for the Femto Network Gateway (FNG) to interface with the Femto Access Points (FAPs) in the network.



aaa aggregation

Sets the system attributes for A12 aggregation for the FNG service.

Product

FNG

Privilege

Security Administrator, Administrator

Syntax

aaa aggregation { interface type *a12*| **destination address** *ipv4_address* | **a12-group { context** *name* **[aaa-group** *name* **] | aaa-group** *name* **[context** *name* **] } }**

no aaa aggregation interface type *a12*

no a12 destination address *ipv4_address*

no aaa aggregation a12-group { context *name* **[aaa-group** *name* **] | aaa-group** *name* **[context** *name* **] }**

aaa aggregation interface type *a12*

Enables A12 aggregation functionality for the FNG service.

aaa aggregation interface a12 destination address *ipv4_address*

Adds a destination address for an AN-AAA server for A12 aggregation. A maximum of ten destination addresses can be configured.

aaa aggregation a12-group { context *name* **[aaa-group** *name* **] | aaa-group [context** *name* **] }**

Defines the AAA context and AAA group to be used for A12 aggregation.
If the context name and AAA group are not specified, the FNG defaults to the FNG service context and the default AAA group in that context. If the AAA group is specified but the context is not specified, the FNG uses the FNG service context and the AAA group in that context. If the AAA group is not specified and the context is specified, the FNG uses the default AAA group in that context.

no aaa aggregation interface type *a12*

Disables A12 aggregation functionality for the FNG service.

no aaa aggregation a12-destination address *ipv4_address*

Deletes the specified destination address for an AN-AAA server.

no aaa aggregation a12-group { context *name* **[aaa-group** *name* **] | aaa-group [context** *name* **] }**

Deletes the specified AAA context and AAA group to be used for A12 aggregation.

Usage

Sets the system attributes for AAA aggregation in the FNG service.

Example

The following command enables the A12 functionality for the FNG service:

```
aggregation interface type a12
```

aaa authentication

Specifies the AAA group to use for FAP authentication.

Product

FNG

Privilege

Security Administrator, Administrator

Syntax

```
aaa authentication { context-name name aaa-group name | context-name name aaa-group name }

no aaa authentication
```

no aaa authentication

Removes any existing authentication configuration.

context-name *name* **aaa-group** *name*

Specifies the context name and the AAA group name configured in the context for FAP authentication.
context-name *name*: Specifies the context where the AAA server group is defined as an alphanumeric string of 1 through 79 characters.
aaa-group *name*: Specifies the name of the AAA group to be used for authentication as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify that during IPSec session establishment using IKEv2 setup, the FNG will use Radius AAA for FAP authentication.

Example

Use the following to configure device authentication for an AAA group named *aaa-10* in the FNG context named *fng1*:

```
aaa authentication context-name fng1 aaa-group aaa-10
```

bind

Binds the FNG service IP address to a crypto template and specifies the maximum number of sessions the FNG service supports.

Product

FNG

Privilege

Security Administrator, Administrator

Syntax

bind address *ipv4_address* **{ crypto-template** *string* **}[max-sessions** *number* **]**

no bind

no bind

Removes a previously configured binding.

address *ipv4_address*

Specifies the IPv4 address of the FNG service.

crypto-template *string*

Specifies the name of the crypto template to be bound to the FNG service.
string is any value from 0 - 127 alpha and/or numeric characters.

max-sessions *number*

Specifies the maximum number of sessions to be supported by the FNG service as an integer from 0 through 1000000. Default: 1000000
If the max-sessions value is changed on an existing system, the new value takes effect immediately if it is higher than the current value. If the new value is lower than the current value, existing sessions remain established, but no new sessions are permitted until usage falls below the newly-configured value.

Usage

Binds the IP address used as the connection point for establishing the IKEv2 sessions to a crypto template. It can also define the maximum number of sessions the FNG can support.

Example

The following command binds an FNG service with an IP address of *10.2.3.4* to the crypto template named *T1* and sets the maximum number of sessions to *500000*:

```
bind address 10.2.3.4 crypto-template T1 max-sessions 500000
```

default

Sets or restores the default condition for the selected parameter.

Product

FNG

Privilege

Security Administrator, Administrator

Syntax

default { { aaa attribute 3gpp2-service-option } | duplicate-session-detection | ip source-violation { drop-limit | period } | setup-timeout | subscriber *name* **}**

aaa attribute 3gpp2-service-option

Sets or restores the default value of 4095.

duplicate-session-detection

Sets or restores the default option for duplicate session detection to be fapid-based.

ip source-violation (drop-limit | period }

Sets or restores the IP source violation detection defaults, as follows:
drop-limit: Sets or restores the maximum number of IP source violations within the detection period before dropping the call to the default value of 10.
period: Sets or restores the detection period for IP source violations to the default value of 120 seconds.

setup-timeout

Sets or restores the maximum time allowed for session setup to the default value of 60 seconds.

subscriber *name*

Sets or restores the name of the default subscriber.
name is a string of 1-127 characters.

username mac-address-stripping

The default behavior is to disable stripping the MAC address from the username.

Usage

Configures the default settings for a given parameter.

Example

Use the following command to set the maximum time allowed for session setup to the default value of 60 seconds:

```
default setup-timeout
```

duplicate-session-detection

Configures the FNG to detect duplicate call sessions based on Femtocell Access Point (FAP) ID and to clear old call information.

This feature is disabled by default.

Product

FNG

Privilege

Security Administrator, Administrator

Syntax

```
duplicate-session-detection { fapid-based }

no duplicate-session-detection

default duplicate-session-detection
```

fapid-based

Sets the FNG to detect duplicate call sessions based on the FAP ID.

no duplicate-session-detection

Disables duplicate session detection.

default duplicate-session-detection

Sets or restores the default option for duplicate session detection to be fapid-based.

Usage

By default, duplicate session detection is disabled.Use this command to enable this feature. It applies only to calls established after the feature has been enabled.
The following command enables duplicate session detection based on FAP ID:

```
duplicate-session-detection fapid-based
```

ip source-violation

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

Product

FNG

Privilege

Security Administrator, Administrator

Syntax

ip source-violation { clear-on-valid-packet | drop-limit *num* **| period** *secs* **}**

no ip source-violation clear-on-valid-packet

clear-on-valid-packet

Configures the service to reset the drop-limit counters upon receipt of a properly addressed packet. Default: disabled

drop-limit *num*

Sets the maximum number of allowed IP source violations within the detection period before dropping a call as an integer from 1 through 1000000. Default: 10

period *secs*

Sets the detection period (in seconds) for IP source violations as an integer from 1 through 1000000. Default: 120

Usage

This function allows the operator to configure the network to prevent problems such as when a user gets handed back and forth between two gateways a number of times during a handoff scenario.
When a subscriber packet is received with a source IP address violation, the system increments the IP source violation drop-limit counter and starts the timer for the IP source violation period. Every subsequent packet received with a bad source address during the IP source violation period causes the drop-limit counter to increment.
For example, if the drop-limit is set to 10, after 10 source violations, the call is dropped. The detection period timer continues to count throughout this process.

Example

The following command sets the drop limit to *15* and leaves the other values at their default values:

```
ip source-violation drop-limit 15
```

setup-timeout

Specifies the maximum time allowed to set up a session in seconds.

Product

FNG

Privilege

Security-Administrator, Administrator

Syntax

setup-timeout *integer*

default setup-timeout

setup-timeout *integer*

Sets the session setup timer (in seconds) as an integer from 2 through 300. Default: 60

default

Sets or restores the default session setup timer value to 60 seconds.

Usage

The FNG clears both the user session and tunnels if a call does not initiate successfully before the session setup timer expires.

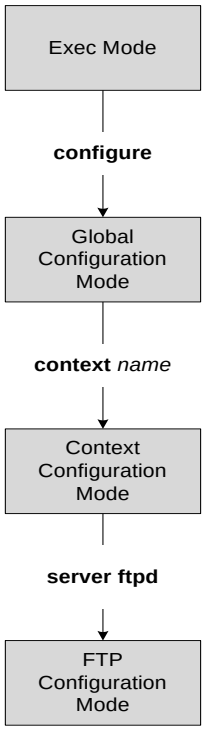
Example

The following command sets the session setup timeout value to the default value of 60 seconds:

```
default setup-timeout
```

Chapter 125
FTP Configuration Mode Commands

The FTP Configuration Mode is used to manage the FTP server options for the current context.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

max servers

Configures the maximum number of FTP servers that can be started within any 60 second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

Product

All

Privilege

Security Administrator, Administrator

Syntax

max servers *count*

count

Default: 40
Specifies the maximum number of servers that can be spawned in any 60-second interval. *count* must be an integer from 1 through 100.

Usage

Set the number of servers to tune the system response as a heavily loaded system may need more servers to support the incoming requests.
The converse would be true as well in that a system can benefit by reducing the number of servers such that FTP services do not cause excessive system impact to other services.

Example

```
max servers 50
```

timeout

Configures the client idle timeout before an FTP session is automatically closed.

Product

All

Privilege

Security Administrator, Administrator

Syntax

timeout *seconds*

seconds

Default: 900
Specifies the number of seconds of inactivity before an FTP session is automatically closed. *seconds* must be an integer from 10 through 86400.

Usage

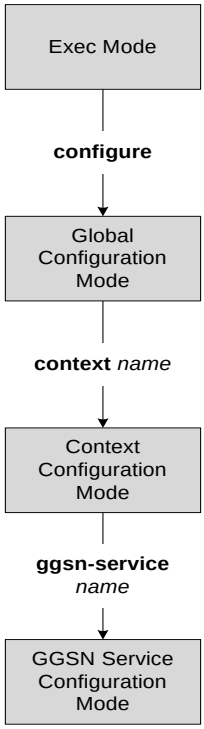
Adjust the session timeout to fine tune the system. FTP session resources can be released sooner to support additional requests by adjusting the timeout to a smaller value.

Example

```
timeout 300
```

Chapter 126
GGSN Service Configuration Mode Commands

The Gateway GPRS Support Node (GGSN) Configuration Mode is used to create and manage GGSN services within the current context.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

accounting

Configures the name of the context configured on the system that processes accounting for PDP contexts handled by this GGSN service.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

accounting context *context_name*

no accounting context

no

Removes a previously configured accounting context.

context_name

Specifies the name of the context to be used for accounting. *context_name* must be an alphanumeric string of 1 through 79 characters that is case sensitive.

Usage

By default, the system attempts to use the same context as the one in which the GGSN service is configured for accounting purposes. This command can be used to either change the system's default behavior, or allow GPRS Tunneling Protocol Prime (GTPP) accounting to a charging gateway (CG).
By default when GTPP accounting is used, accounting records will be sent to the accounting servers configured in whichever context the GGSN service is configured. This command may be used to override that default.

Example

The following command configures the GGSN service's accounting context to be plmn1:

```
accounting context plmn1
```

associate gtpu-service

This command associates a previously configured GTP-U service to bind the GGSN service with a peer. A GTP-U service must be configured in Context Configuration mode before using this configuration.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

associate gtpu-service *svc_name*

noassociate gtpu-service

no

Removes the associated GTP-U service from this GGSN service configuration.

svc_name

Identifies the name of the GTP-U service preconfigured in Context Configuration mode to associate with a GGSN service. *svc_name* is an alphanumeric string from 1 through 63 characters.

Usage

Use this command to configure GTP-U data plan between GGSN service and peer node. The service defined for GTP-U can be configured in Context configuration mode.

Example

Following command associates GTP-U service named *gtpu-hnb1* with specific GGSN service.

```
associate gtpu-service gtpu-hnb1
```

associate pgw-service

This command enables a previously configured P-GW service to which handover will be done by the GGSN service. The P-GW service must be configured in Context Configuration mode before using this configuration.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

associate pgw-service *svc_name*

no associate pgw-service

no

Removes the associated P-GW service from this GGSN service configuration.

svc_name

Identifies the name of the P-GW service preconfigured in Context Configuration mode to which handover will be done.
The *svc_name* must be an alphanumeric string from 1 through 63 characters.

Usage

Use this command to allow enabling/disabling bearer handover from GGSN to a P-GW service. The service defined for P-GW can be configured in Context configuration mode.
The P-GW's eGTP service should have the same bind address as GGSN service and P-GW and GGSN should share same GTP-U, otherwise handover will fail.

Example

Following command enables P-GW service named *pgw-test* handover with specific GGSN service.

```
associate pgw-service pgw-test
```

authorize-with-hss

This command enables or disables subscriber session authorization via a Home Subscriber Server (HSS) over an S6b Diameter interface. This feature is required to support the interworking of GGSN with P-GW and HA.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
authorize-with-hss[ report-ipv6-addr ]

[ default | no ] authorize-with-hss
```

no

Disables the default authorization of subscriber over S6b interface. Resets the command to the default setting of "authorize locally" from an internal APN authorization configuration.

report-ipv6-addr

Enables the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface.

Usage

Use this command to enable/disable the authorization support for subscriber over S6b interface, which is used between GGSN and the 3GPP AAA to exchange the information related to charging, P-CSCF discovery, etc. By use of this feature allows the GGSN service to interact with HSS over S6b interface through Diameter configuration which is already configured on the system.

Important: Diameter configuration must be available before enabling this command. For more information of Diameter interface configuration, refer *Diameter Endpoint Configuration Mode Commands* chapter.

Important: This command is a license-enabled feature.

Example

The following command enables the subscriber authorization via an HSS over an S6b Diameter interface to provide session interoperability between GGSN and PGW and HA in this GGSN service:

```
authorize-with-hss
```

bind

Binds the GGSN service to a logical IP interface serving as the Gn interface. Specifies the maximum number of subscribers that can access this service over the interface.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

bind address *ip_address* **max** [**total-pdp-contexts** *max_total* | **ppp-pdp-contexts** *max_ppp*]

no bind address *address*

no

Removes a previously configured binding for the GGSN service.

ip_address

Specifies the IP address (address) of the interface configured as the Gn interface. *ip_address* is specified in IPv4 dotted-decimal notation.

max

Configures the maximum limits for total/PPP PDP contexts.

total-pdp-contexts *max_total*

Default: 1500000
Specifies the maximum number of PDP contexts (both IP and PPP) that can access this service on this interface.
count is an integer from 0 through 4000000.

Important: The maximum number of supported subscriber contexts varies based on the installed session capacity license and the number of active packet processing cards installed in the system. Note that each PPP PDP context is treated as two IP PDP contexts. Refer to the **license key** command for additional information.

ppp-pdp-contexts *max_ppp*

Default: 750000
Specifies the maximum number of PPP PDP contexts that can access this service on this interface.
count can be configured to an integer from 0 and 2500000.

Important: The maximum number of supported subscriber contexts varies based on the installed session capacity license and the number of active packet processing cards installed in the system. Refer to the **license key** command for additional information.

Usage

Used to associate or tie the GGSN service to a specific logical IP address. The logical IP address or interface takes on the characteristics of a Gn interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a "soft" limit as to the number of simultaneous subscriber contexts that can be facilitated by the service/interface at any given time. Soft limits are based on measurements gathered at regular short intervals (several times per minute) as opposed to measurements taken in real-time. Therefore, the sampled measurement may not match the actual number of PDP contexts currently being processed. Every PDP context request received is compared against the result of the last sample. If the sample is less than the soft limit configured, the request will be processed. If it is more, the request will be rejected.

When configuring the **`total-pdp-contexts`** or **`ppp-pdp-contexts`** options, be sure to consider the following:

- Each PPP PDP context is treated as two IP PDP contexts due to the additional CPU and memory resources required
- The total number of configured Gn interfaces
- The maximum number of subscriber PDP contexts that all of the interfaces may handle during peak busy hours
- The average bandwidth for each of the PDP contexts
- The type of physical port (10/100Base-T or 1000Base-Tx) to which these interfaces are bound

Taking these factors into account and distributing your subscriber contexts across all available interfaces allows you to configure your interfaces to optimally handle PDP contexts without degrading performance.

Example

The following command would bind the logical IP interface with the address of *`192.168.3.1`* to the GGSN service and specifies that a maximum of *`600`* simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 192.168.3.1 max-subscribers 600
```

The following command disables a binding that was previously configured:

```
no bind address
```

cc behavior

Configures the 3GPP behavior bits associated with the GGSN's charging characteristics (CC).

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
cc behavior no-records nr_value

default cc behavior

no cc behavior no-records
```

no-records *nr_value*

Default: 0 (disabled)
Specifies the behavior bit upon which the GGSN ceases sending accounting records to a server.
nr_value can be configured to an integer from 1 through 12 corresponding to the 12 behavior bits – B1 through B12.

Usage

3GPP standards after 3GPP R98 included 12 behavior bits as part of GGSN charging characteristics. Like the charging characteristics profile index, the behavior bits are sent by the SGSN to the GGSN in the Create PDP Context request message.
This command configures the behavior bits for each of the conditions described.

Example

The following command configures a behavior bit of 10 for no-records:

```
cc behavior no-records 10
```

cc profile

Configures the charging characteristic (CC) profile index properties.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

cc profile *index* [**buckets** *number* | **interval** *time* [**downlink** *down_octets* **uplink** *up_octets* | **total** *total_octets*] | **prepaid** { **prohibited** | **use-rulebase-configuration** } | **sgsns** *num_changes* | **tariff time1** *mins hours* [**time2** *mins hours* [**time3** *mins hours* [**time4** *mins hours* [**time5** *mins hours* [**time6** *mins hours*]]]] | **volume** { **downlink** *vol_down_octets* **uplink** *vol_up_octets* | **total** *total_octets* }]

no cc profile *index* { **buckets** | **interval** | **prepaid** | **sgsns** | **tariff** | **volume** }

default cc profile *index*

no

Removes a previously configured profile index.

default

Returns the specified cc profile to the original default system settings.

index

Configures a profile index for the parameter to be specified. index can be configured to an integer from 0 through 15.

Important: 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

buckets *number*

Default: 4
Specifies the number of statistics container changes due to QoS changes or tariff time that can occur before an accounting record should be closed.
number can be configured to an integer from 1 through 4.

interval *time* **[downlink** *down_octets* **uplink** *up_octets* **| total** *total_octets* **]**

Specifies the normal time duration that must elapse before closing an accounting record provided that any or all of the following conditions occur:

- Downlink traffic volume is reached within the time interval
- Uplink traffic volume is reached within the time interval
- Total traffic volume (up and downlink) is reached within the time interval

time is measured in seconds and can be configured to an integer from 60 through 40000000.
down_octets is the downlink traffic volume measured in octets and can be configured to an integer from 0 through 1000000.
up_octets is the uplink traffic volume measured in octets and can be configured to an integer from 0 through 1000000.
total_octets is the total traffic volume measured in octets and can be configured to an integer from 0 through 1000000.

prepaid { prohibited | use-rulebase-configuration }

This command enables or disables prepaid for the specified profile index.
Default: N/A
prohibited: Disable prepaid for the specified profile index.
use-rulebase-configuration: Use the prepaid configuration in the rulebase.

sgsns *num_changes*

Default: 4
Specifies the number of SGSN changes (such as, inter-SGSN switchovers) resulting in a new RAI (Routing Area Identity) that can occur before closing an accounting record.
num_changes can be configured to an integer from 1 through 15.

tariff time1 *mins hours* **time2** *mins hours* **time3** *mins hours* **time4** *mins hours* **time5** *mins hours* **time6** *mins hours*

Specifies time-of-day time values to close the current statistics container (but not necessarily the accounting record). Six different tariff times may be specified. If less than six times are required, the same time can be specified multiple times.

Important: The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

For each of the different tariff times, the following parameters must be configured:

- *mins*: The minutes of the hour, an integer value from 0 to 59.
- *hours*: The hour of the day, an integer value from 0 to 23.

volume {downlink *vol_down_octets* **uplink** *vol_up_octets* **| total** *total_octets* **}**

Specifies the downlink, uplink, and total volumes that must be met before closing an accounting record.
vol_down_octets is measured in octets and can be configured to an integer from 100000 to 4000000000.
vol_up_octets is measured in octets and can be configured to an integer from 100000 to 4000000000.
total_octets is the total traffic volume (up and downlink) measured in octets and can be configured to an integer from 100000 to 4000000000.

Usage

Charging characteristics consist of a profile index and behavior settings. This command configures profile indexes for the GGSN's charging characteristics. The GGSN supports up to 16 profile indexes.
This command works in conjunction with the **cc-sgsn** command located in the APN Configuration Mode that dictates which CCs should be used for subscriber PDP contexts.

Example

The following command configures a profile index of *10* for tariff times of 7:00 AM and 7:30 PM:

```
cc profile 10 tariff time1 0 7 time2 30 19 time3 0 7 time4 30 19
```

default

Sets/restores the default value assigned for the specified parameter.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default ] { cc { behavior | profile index } | echo-interval | gtpu echo-interval | gtpu
reorder { context | sequence-numbers | timeout } | guard-interval | ip { local-port gtpc-
v1 | qos-dscp } | max-retransmissions | plmn { unlisted-sgsn } | setup-timeout | timeout
}
```

---

cc { behavior | profile *index* }

Restores the GGSN's charging characteristics parameters to the following default settings:

- **behavior**: Restores all behavior parameters to their default values of 0 (disabled).
- **profile:** For the specified index, the following defaults are applied:
  - buckets: 4
  - interval: Disabled
  - volume: Disabled
  - sgsns: 4
  - tariff-time: Disabled

---

echo-interval

Restores the GTP echo-interval parameter to its default setting of 60.

---

gtpu echo-interval

Restores the GTPU echo-interval parameter to its default setting of 60.

---

gtpu reorder {context | sequence-numbers | timeout }

Restores the gtpu reordering parameters to the following default settings:

- gtpu reorder context: Disabled
- gtpu reorder sequence-numbers: Disabled
- gtpu reorder timeout: 100 milliseconds

---

gtpu udp-checksum insert

Restores the GGSN gtpu udp-checksum parameter to its default setting of enabled.

---

guard-interval

Restores the GGSN guard-interval parameter to its default setting of 100.

ip {local-port gtpc-v1 | qos-dscp }

Restores the GGSN ip parameters to the following default setting:

- **local-port gtpc-v1**: 2123
- **qos-dscp**: conversational ef streaming af11 interactive af21 background be

max-retransmissions

Restores the GGSN max-retransmissions parameter to its default setting of 4.

plmn {unlisted-sgsn }

Restores the GGSN plmn unlisted-ggsn parameter to its default setting of reject.

setup-timeout

Restores the GGSN setup-timeout parameter to its default setting of 60.

timeout

Restores the GGSN timeout parameter to its default setting of 5.

Usage

After the system has been modified from its default values, this command is used to set/restore specific parameters to their default values.

Example

The following command restores the GGSN service's guard interval parameter to its default setting:

```
default guard-interval
```

dns-client

This command defines the context name where a DNS client is configured. It associates an existing DNS client configuration with the GGSN to perform a DNS query for P-CSCF, if a P-CSCF query request in an AAA message is received from the Diameter node.

Product

All

Privilege

Security Administrator, Administrator

Syntax

dns-client context *dns_ctxt_name*

[**no** | **default**] **dns-client context**

no

Removes the association of DNS context which was configured to perform DSN query in this GGSN service.

default

Sets the default context for the DNS client.

dns_ctxt_name

Specifies the name of the context in which a DNS client configuration is present. Typically this should be the same context in which this GGSN service is configured.
dns_ctxt_name is a context name and must be alphanumeric string of 1 through 79 characters.

Usage

Use this command to associate a DNS client configuration to perform DNS query used for the resolution of P-CSCF query received in AAA message from Diameter peer, on the basis of DNS client parameters configured in a context.
A DNS client configuration must be present in the same context as GGSN service before enabling this command to perform DNS query for P-CSCF.

Important: This command is a license-enabled feature.

Example

The following command associates a DNS client configuration to perform DNS query for P-CSCF with this GGSN service which is configured in same context as GGSN service:

```
default dns-client context
```

echo-interval

Configures the rate at which GPRS Tunneling Protocol (GTP) v1-C Echo packets are sent from the GGSN service to the SGSN.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

echo-interval *time_interval*

[**default** | **no**] **echo-interval**

default

Configures the default value (60 seconds) for echo interval.

no

Disables the sending of GTPv1-C Echo packets.

time_interval

Default: 60
Specifies the frequency at which the GGSN service sends GTPv1-C Echo packets to the SGSN(s) it is configured to communicate with.
time_interval is measured in seconds and can be configured to an integer from 60 through 3600.

Usage

Use this command to adjust the rate at which the GGSN sends these packets. GTPv1-C Echo packets are used to detect whether SGSNs that the GGSN service is communicating with, has become unresponsive or has rebooted.
The system initiates this protocol for each of the following scenarios:

- Upon system boot
- Upon the configuration of a new SGSN on the system using the **sgsn address** command as described in this chapter
- Upon the execution of the path failure detection policy as described in **path-failure** command of this chapter

The echo-interval command is used in conjunction with the **max-retransmissions** and **retransmission-timeout** commands as described in this chapter.
In addition to receiving an echo response for this echo protocol, if GGSN receives a Node Alive Request message or a Echo Request message from a presumed dead SGSN, it will immediately assume the SGSN is active again.
If the GGSN discovers that an SGSN has become unresponsive, it will terminate all PDP contexts that had been established with the SGSN.

Example

The following command configures the GGSN service to send GTP Echo packets every 120 seconds:

```
echo-interval 120
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

fqdn

This command defines Fully Qualified Domain Name (FQDN) which would be used for authorization over S6b interface between GGSN and 3GPP AAA/HSS.

Product

All

Privilege

Security Administrator, Administrator

Syntax

fqdn host *host_name* **realm** *realm_id*

[**no** | **default**] **fqdn**

no

Removes the configured FQDN host name and realm ID from the GGSN service.

default

Sets the system to default mode for this command and configures the host and realm ID value to NULL.

host *host_name*

Specifies the name of the host to be used for authorization over an S6b interface to a 3GPP AAA server/HSS from the GGSN service.
host_name is a unique node name for authorization over the S6b interface from this GGSN service.
host_name must be an alphanumeric string of 1 through 127 characters. Punctuation marks are allowed.

realm *realm_id*

Specifies the realm as an FQDN to be used for authorization over S6b interface with 3GPP AAA server/HSS from GGSN service. The realm may typically be a company or service name.
realm_id is a unique identifier configured for the authorization over S6b interface from this GGSN service, expressed as an alphanumeric string of 1 through 127 characters. Punctuation marks are allowed.
host_name

Usage

Use this command to define host and realm as the FQDN for a 3GPP AAA server/HSS that would be used for authorization over an S6b interface with the GGSN. The realm specified as an FQDN may typically be a company or service name.
By default the FQDN host and realm will be NULL

Important: This command is a license-enabled feature.

Example

The following configures the *hss1* as host name and *xyz.com* as realm to support authorization over an S6b from this GGSN service:

```
fqdn host hss1 realm xyz.com
```

gtpc nsapi-in-create-pdp-response

This command excludes or includes the optional information element (IE) Network Service Access Point Identifier (NSAPI) within “Create PDP Context Response” messages in GTP-C.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] gtpc nsapi-in-create-pdp-response
```

default

Sets the default mode for GTP-C messages not to include the NSAPI IE in “Create PDP Context Response” messages.

no

Removes the preconfigured mode for GTP-C messages; the GTP-C message will not include the NSAPI IE in “Create PDP Context Response” messages. By default it is disabled.

Usage

Use this command to exclude or include the NSAPI IE in “Create PDP Context Response” GTP-C messages received from the SGSN.

Example

The following command configures the GGSN service to include the optional NSAPI IE in “Create PDP Context Response” messages:

```
gtpc nsapi-in-create-pdp-response
```

gtpc private-extension

This command includes customer-specific private extensions in GTP-C messages.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpc private-extension { { { focs | odb } access-list acl_name in disconnect-on-violation
} | ggsn-preservation-mode | loss-of-radio-coverage | none }

default gtpc private-extension

no gtpc private-extension [ focs | ggsn-preservation-mode | loss-of-radio-coverage ]
```

default

Sets the default mode for GTP-C messages. By default it is disabled.

no

Disables the configured private extensions for GTP-C messages.

{focs | odb} access-list *acl_name* **in disconnect-on-violation**

Configures the Free-Of-Charge-Service (FOCS) and Operator Determined Barring (ODB) extensions for all packet-oriented services as defined by operators.
focs: Enables or disables Free of Charge Services for the subscriber who has no credit, and also takes the access-list *acl_name* to be applied for FOCS.
odb: Enables or disables "all packet oriented service barred" for the subscriber, and also takes the access-list *acl_name* to be applied for ODB.
acl_name is the name of a configured access control list (ACL) for this service.

Important: These are the customer-specific keywords and need customer-specific license to use them.

ggsn-preservation-mode

Enables the processing of customer-specific private extension in Update PDP Context requests. This extension indicates whether the subscriber is active or idle, and whether RAN resources have been released. It also indicates the desired "type" of preservation mode behavior.
When **ggsn-preservation-mode** is configured, different types of accounting records are generated based on the "type" of mode. To enable the generation of different accounting records, the trigger for preservation mode must be configured for RADIUS or GTPP for that accounting protocol. If that trigger is not configured, there will be no change in the generation of accounting records.

Important: This is a customer-specific keyword and needs customer-specific license to use this feature.

loss-of-radio-coverage

Enables the protection against overcharging a subscriber due to loss of radio coverage (LORC) in a GGSN service. It also enables the system to understand the private extension for LORC) in GTP-C Update PDP Context messages from the SGSN.

Important: This is a license enabled keyword and need feature-specific license to use it.

none

Removes the private extensions from record which are from GTP-C messages received from the SGSN.

Usage

Use this command to configure the processing of private extensions within GTP-C messages received from the SGSN. It also configures the customer specific features, such as preservation mode for GGSN service. Overcharging protection (LORC) is a solution which provides the ability to accurately bill customers. This implementation is based on Cisco-specific private extension to GTP messages and/or any co-relation of G-CDRs and S-CDRs. It also does not modify any RANAP messages.

Important: This is a license enabled command that requires installation of feature-specific licenses to use this command.

Example

The following command configures the GGSN service to record the private extension for protecting the subscribers from overcharging during loss of radio coverage:

```
gtpc private-extension loss-of-radio-coverage
```

gtpc ran-procedure-ready-delay

This command configures the GGSN to enable the RAN Procedure Ready feature for the particular GGSN service and specify the timeout period for the RAN procedure timer in the GGSN. This timer starts on arrival of every secondary Create PDP Context request.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

gtpc ran-procedure-ready-delay [**timeout** *dur*]

[**default** | **no**] **gtpc ran-procedure-ready-delay**

default

Sets the default mode of RAN Procedure Ready feature for this GGSN service. By default it is disabled.

no

Disables the RAN Procedure Ready feature for this GGSN service. By default it is disabled.

timeout *dur*

Default: 10
Specifies the timeout duration (in seconds) for the RAN procedure timer. This timer starts on the arrival of every secondary "Create PDP Context Request" message.
This is an optional keyword. If no timeout period is specified, the default value is 10 seconds.
dur must be an integer from 1 through 40.

Usage

Use this command to enable the RAN Procedure Ready feature for this GGSN service and specify the timeout period for the RAN procedure timer. This timer starts on the arrival of every secondary "Create PDP Context Request" message.
The GGSN waits until the Radio Access Bearer setup is completed and "Update PDP Context Request" is sent by the SGSN. If any downlink data is received before arrival of the "Update PDP Context Request" or before timer expiry, the downlink packets will be queued or buffered.
If the buffer becomes full (total buffer limit is of 1024 packets), all newly arriving packets are dropped.
The RAN Procedure Ready feature supports the following scenarios when RAB setup timer starts at the GGSN:

- If the GGSN receives the "Update PDP Context Request" before timer expiry, the GGSN stops the timer, sends all the queued/buffered packets in 'first-in first-out' manner and disables buffering of subsequent downlink data.
- If the GGSN receives the "Update PDP Context Request" before the timer expires, it processes the "Update PDP Context Request" as usual, but does not disable the buffering of downlink data. It then waits for another "Update PDP Context Request" to come with the RAN Procedure Ready set, or waits for timer to expire.

- If the GGSN does not receive the "Update PDP Context Request" with RAN Procedure Ready set before timer expiry, the timer is fired and the GGSN starts sending all queued packets and disables buffering of subsequent downlink data (assuming that the corresponding SGSN does not support this feature).
- If the timer has expired and the GGSN receives an "Update PDP Context Request" for a secondary PDP context with or without RAN Procedure Ready bit set, the UPC will be processed normally without buffering the packets.

Important: This feature does not affect the Enhanced Charging Service or deep packet inspection (DPI) since the buffering of downlink data is done before sending it to an ACSMgr.

Important: During an SGSN handoff scenario all packets are processed normally and the downlink packets are buffered until the timer expires.

Example

The following command configures the GGSN service to enable the RAN Procedure Ready feature and specify the timeout period as *20* seconds for the RAN Procedure timer in GGSN:

```
gtpc ran-procedure-ready-delay timeout 20
```

gtpu echo-interval

This command is obsolete and now available for configuration in GTP-U service configuration mode.

guard-interval

Configures the time period after which a redundant PDP context request received from an SGSN is treated as a new request rather than a re-send of a previous request.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

guard-interval *guard_time*

[**default** | **no**] **guard-interval**

default

Configures the default value for guard-interval function for the GGSN service.

no

Disables the guard-interval function for the GGSN service.

guard_time

Default: 100
Specifies the amount of time that must pass before a GGSN service treats a redundant PDP context request as a new request instead of a re-send of a previous request.
guard_time is measured in seconds and can be configured to an integer from 10 through 3600.

Usage

The guard interval is used to protect against replay attacks. Without a guard interval configured, information from a valid PDP context request could be used to gain un-authorized network access.
If the GGSN service receives a PDP context request in which the International Mobile Subscriber Identity (IMSI), the Network Service Access Point Identifier (NSAPI), the end user IP address, and the GTP sequence number are identical to those received in a previous request, the GGSN treats the new request as a re-send of the original. Therefore, information from a valid PDP context request could be collected and re-sent at a later time by an un-authorized user to gain network access.
Configuring a guard interval limits the amount of time that the information contained within a PDP context request remains valid.

Example

The following command configures the GGSN service with a guard interval of *60* seconds:

```
guard-interval 60
```

ip local-port

Configures the local User Datagram Protocol (UDP) port for the Gn interfaces' GTP-C socket for GTPv1.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
ip local-port gtpc-v1 port#

default ip local-port gtpc-v1
```

default

Configures the default value for the local UDP port for GTP Version 1 control messaging for this GGSN service.

gtpc-v1 *port#*

Default: 2123
Specifies the UDP port number for GTPv1 GTPC sockets.
port# can be configured to an integer from 1 through 65535.

Usage

By default, the GGSN service attempts to use GTPv1 when communicating with SGSNs. This parameter configures the UDP port over which the GTP control (GTP-C) sockets are sent.
If an SGSN only supports GTPv0, the GGSN service automatically switches to GTPv0 when communicating with this SGSN. In the scenario, the GGSN service communicates with the SGSN on UDP port 3386 and does not have a GTP-C socket.

Important: The UDP port setting on the SGSN must match the local-port setting for the GGSN service on the system in order for the two devices to communicate.

Example

The following command configures the GGSN service to use UDP port *2500* for exchanging GTPC sockets with SGSNs when using GTPv1:

```
ip local port 2500
```

ip qos-dscp

Configures the quality of service (QOS) differentiated service code point (DSCP) used when sending data packets over the Gn interface.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
ip qos-dscp { qci { 1 { dscp } | 2 { dscp } | 3 { dscp } | 4 { dscp } | 5 { dscp |
allocation-retention-priority } | 6 { dscp | allocation-retention-priority } | 7 { dscp |
allocation-retention-priority } | 8 { dscp | allocation-retention-priority } | 9 { dscp
}} | gtpc } +

no ip qos-dscp { qci { 1 | 2 | 3 | 4 | 5 { allocation-retention-priority | dscp } | 6 {
allocation-retention-priority | dscp } | 7 { allocation-retention-priority | dscp } | 8 {
allocation-retention-priority | dscp } | 9 } | gtpc } +
```

allocation-retention-priority

Specifies the DSCP for interactive class if the allocation priority is present in the QOS profile.
allocation-retention-priority can be the integer 1, 2, or 3.
DSCP values use the following matrix to map based on traffic handling priority and Alloc/Retention priority if the allocation priority is present in the QOS profile.
The following table shows the DSCP value matrix for *allocation-retention-priority*.

Table 19. Default DSCP Value Matrix

Allocation Priority	1	2	3
Traffic Handling Priority			
1	ef	ef	ef
2	ef	ef	ef
3	af21	af21	af21
	af21	af21	af21

qci

Configures the QoS Class Identifier (QCI) attribute of QOS. Here the *qci_val* is the QCI for which the negotiate limit is being set; it ranges from 1 to 9.

dscp

Default QCI:
- 1: ef

- 2: ef
- 3: af11
- 4: af11
- 5: ef
- 6: ef
- 7: af21
- 8: af21
- 9: be

Specifies the DSCP for the specified traffic pattern. *dscp* can be configured to any one of the following:

• **af11:** Assured Forwarding 11 per-hop-behavior (PHB)	• **af32:** Assured Forwarding 32 PHB
• **af12:** Assured Forwarding 12 PHB	• **af33:** Assured Forwarding 33 PHB
• **af13:** Assured Forwarding 13 PHB	• **af41:** Assured Forwarding 41 PHB
• **af21:** Assured Forwarding 21 PHB	• **af42:** Assured Forwarding 42 PHB
• **af22:** Assured Forwarding 22 PHB	• **af43:** Assured Forwarding 43 PHB
• **af23:** Assured Forwarding 23 PHB	• **be:** Best effort forwarding PHB
• **af31:** Assured Forwarding 31 PHB	• **ef:** Expedited forwarding PHB

+

More than one of the above keywords can be entered within a single command.

Usage

DSCP levels can be assigned to specific traffic patterns in order to ensure that data packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the outer IP header of every GTP data packet. The diffserv marking of the inner IP header is not modified.
The traffic patterns are defined by QCI (1 to 9). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in the following tables:

Table 20. Class structure for assured forwarding (af) levels

Drop Precedence	Class			
	Class 1	Class 2	Class 3	Class 4
Low	af11	af21	af31	af41
Medium	af12	af22	af32	af41
High	af13	af23	af33	af43

Table 21. DSCP Precedence

Precedence (low to high)	DSCP
0	Best Effort (be)
1	Class 1
2	Class 2
3	Class 3
4	Class 4
5	Express Forwarding (ef)

The DSCP level can be configured for multiple traffic patterns within a single instance of this command. The **no ip qos** command can be issued to remove a QOS setting and return it to it's default setting.

Example

The following command configures the DSCP level for QCI to be Expedited Forwarding,**ef**:

```
ip qos-dscp qci 1 ef
```

max-retransmissions

Configures the maximum number of times that GTP control packets are retransmitted to an SGSN before it marks it unreachable.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
max-retransmissions max_number

default max-retransmissions
```

default

Configures the default value for maximum retries for GTP control packets for the GGSN service.

max_number

Default: 4
Indicates the maximum number of times that GTP control packets are retransmitted.
max_number can be configured to an integer from 0 through 15.

Usage

This command is used in conjunction with the **timeout** command to control the retransmission of GTP control packets when no response is received from an SGSN. It is equivalent to the N3-REQUESTS parameter discussed in 3GPP TS 29.060.
If no response is received from the SGSN prior to the expiration of the timeout value, the GTP control packets are re-sent by the GGSN. This process occurs as many times as allowed by the configuration of this command.
If the max-retransmissions value is exceeded, the GGSN records a “Path Failure” for that SGSN and releases all PDP contexts associated with it.

Example

The following command configures the maximum number of retransmissions to *8*:

```
max-retransmissions 8
```

mbms policy

This command enables/disables the Multimedia Broadcast Multicast Services (MBMS) user service support for multicast and/or broadcast mode. It also specifies the policy for MBMS user service mode.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
mbms policy { multicst broadcast | none }

[ no | default ] mbms policy
```

no

Removes or disables the configured MBMS support for multicast and/or broadcast mode in this GGSN service.

default

Restores the default mode of MBMS support in this GGSN service.

multicst broadcast

Enables the MBMS support and configures the policy for multicast and broadcast of user service.

Usage

Use this command to enable/disable the MBMS user service support for Multicast and/or Broadcast mode. It also specifies the policy for MBMS user service mode.

Example

The following command enables MBMS support in this GGSN service:

```
mbms policy multicast broadcast
```

newcall

This command enables or disables the new call related behavior of this GGSN service when duplicate sessions with the same IP address request are received. This feature is required to support interworking with P-GW and HA.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
newcall duplicate-subscriber-requested-address { accept | reject }

default newcall duplicate-subscriber-requested-address
```

default

Restores the default mode for new call session with the same address request received in this GGSN service. It rejects calls with duplicate address requests.

accept

Sets the system to "accept" another session using the same IP address for a new call. The new session will be created and the old session will be torn down.
Default: Disabled

reject

Rejects new calls with duplicate address requests. This is the default behavior.
Default: Enabled

Usage

Use this command to enable or disable new call connections when the UE is not able to gracefully disconnect from the Enterprise PDN before attempting to reconnect via another access method. When enabled this command tears down the old session in order to accept the new connection with the same IP address assignment.
This feature also allows the GGSN to accept a request for a static subscriber address, even if the address is already used by another session. If this feature is not enabled, a new request with the same IP address for another session will be rejected.

Important: This command is a license-enabled feature.

Example

The following command allows the GGSN to accept the duplicate call session request with the same IP address:

```
newcall duplicate-subscriber-requested-address accept
```

path-failure

Determines the GTP path-failure behavior on echo/non-echo messages.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
path-failure detection-policy gtp { echo [ non-echo ] | non-echo [ echo ] }

[ no | default ] path-failure detection-policy
```

no

No defined detection policy means path-failures are not detected.

default

Sets the path-failure detection-policy to GTP in echo mode.

detection-policy gtp {echo [non-echo] | non-echo [echo] }

Detection-policy is the policy to be used when path-failure is in active state. GTP messages are either gtp(u) (user) or gtp(c) (control) type, and the gtp keyword takes either echo or non-echo as message type.
echo: gtp(u) or gtp(c) message.
non-echo: a message type other than gtp(u) or gtp(c).

Usage

Under current circumstances, a GGSN shuts down the GTP tunnel if the associated SGSN does not respond to multiple retries of an echo or non-echo message from the GGSN. In this way, a single call failure could be responsible for the loss of all active calls in the tunnel.
This is also an issue when echo is disabled, or when there is very little traffic on the SGSN and the GGSN is configured with large echo intervals.
This behavior adversely impacts the user experience because the customer has to reconnect every time this happens with their SGSN.

Example

The following example detects path failures when the SGSN fails to respond to multiple echo message retries:

```
path-failure detection-policy gtp echo
```

The following example turns off path-failure detection. On timeout of gtp(c) message retries, the particular context will be purged:

```
no path-failure detection-policy
```

plmn id

Configures the GGSN's public land mobile network (PLMN) identifiers. Up to five PLMN IDs can be configured for each GGSN service.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

plmn id mcc *mcc_value***mnc** *mnc_value* [**primary**]

no plmn id mcc *mcc_value* **mnc** *mnc_value*

no

Removes a previously configured PLMN identifier for the GGSN service.

mcc *mcc_value*

Specifies the mobile country code (MCC) portion of the PLMN's identifier.
mcc_number is the PLMN MCC identifier and can be configured to an integer between 100 and 999.

mnc *mnc_value*

Specifies the mobile network code (MNC) portion of the PLMN's identifier.
mnc_number is the PLMN MNC identifier and can be configured to any 2- or 3-digit integer from 00 through 999.

primary

When multiple PLMN IDs are configured, the **primary** keyword can be used to designate one of the PLMN IDs to be used for the AAA attribute (3GPP-GGSN-MCC-MNC).

Usage

The PLMN identifier is used by the GGSN service to determine whether or not a mobile station is visiting, roaming, or home. Multiple GGSN services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each GGSN Service.

Example

The following command configures the PLMN identifier with an MCC of *462* and MNC of *2*:

```
plmn id mcc 462 mnc 02
```

plmn unlisted-sgsn

Configures the GGSN's policy for handling communications from SGSNs with which it is not configured to communicate.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default ] plmn unlisted-sgsn { foreign [ disable-gtpc-echo ] [ reject-foreign-
subscriber ] | home [ disable-gtpc-echo ] | reject | mcc mcc_value mnc mnc_value[
disable-gtpc-echo ] [ reject-foreign-subscriber ] }
```

default

Resets configured parameters to their default settings.

foreign

Default: Disabled
Specifies that the GGSN service accepts messages from SGSNs that are not configured within the service using the **sgsn address** command.
This keyword also dictates that unlisted SGSNs are treated as if they belong to a foreign PLMN. Therefore, PDP contexts originating from them are treated as visiting or roaming.

mcc *mcc_value*

Specifies the mobile country code (MCC) portion of the PLMN's identifier.
mcc_value is the PLMN MCC identifier and can be configured to an integer from 100 through 999.

mnc *mnc_value*

Specifies the mobile network code (MNC) portion of the PLMN's identifier.
mnc_value is the PLMN MNC identifier and can be configured to a 2- or 3-digit integer from 00 through 999.

disable-gtpc-echo

Default: Send GTPC Echo messages to unlisted SGSNs.
When this keyword is specified, GTPC echo messages are not sent to unlisted SGSNs.

reject-foreign-subscriber

Default: Disabled
Specifies that incoming calls from foreign subscribers are rejected.

home

Default: Disabled
Specifies that the GGSN service accepts messages from SGSNs that are not configured within the service using the **sgsn address** command.

This keyword also dictates that unlisted SGSNs are treated as if they belong to the GGSN service's home PLMN.

reject

Default: Enabled
Specifies that the GGSN service rejects messages from SGSNs that are not configured within the service using the **sgsn address** command.
When the GGSN service rejects the message(s), it returns a cause code of No Resources 199 (C7H, No resources available).

Usage

This command works in conjunction with the **sgsn** command that configures the GGSN service to communicate with specific SGSNs. Any messages received from SGSNs not configured in that list are subject to the rules dictated by the **unlisted-sgsn** policy.

Example

The following command configures the GGSN service to accept messages from unlisted SGSNs and treat the SGSN as if it is on the GGSN's home network:

```
plmn unlisted-sgsn accept home
```

policy

Specifies the reject code to be used in the "Create PDP Context" response message when a RADIUS server timeouts.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
policy { accounting-server-timeout use-reject-code { system-failure | no-resources } |
authentication-server-timeout use-reject-code { system-failure | user-authentication-
failure } }

default policy { authentication-server-timeout | accounting-server-timeout }
```

default

Restores the specified parameter to its default setting.

accounting-server-timeout use-reject-code { system-failure | no-resources }

Default: **no-resources**
Specifies the reject code used by the GGSN if communication with an accounting server times out. The possible reject codes are:

- system-failure (204 (CCH))
- no-resources (199 (C7H))

authentication-server-timeout use-reject-code {system-failure | user-authentication-failure }

Default: user-authentication-failure
Specifies the reject code used by the GGSN if communication with an authentication server times out. The possible reject codes are:

- system-failure (204 (CCH))
- user-authentication-failure (209 (D1H))

Usage

This command is used to configure the cause code used by the GGSN if communication with either a RADIUS authentication or accounting server times out.
When this parameter is used in conjunction with Radius accounting servers, the response is only set if a flag is configured in the APN Delay GTP Response, only after getting a response to the Accounting Start.

Example

The following command configures the GGSN response to a RADIUS authentication server timeout to be *system-failure*:

```
policy authentication-server-timeout use-reject-code system-failure
```

retransmission-timeout

Configures the timeout period in between retransmissions of GTP control packets. This timeout configuration is not applicable on Echo Request retransmission.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

retransmission-timeout *retransmit_time*

default retransmission-timeout

default

Configures the default time interval that must pass without an SGSN response before the GGSN service retransmits GTP control packets.

retransmit_time

Default: 5
Specifies the amount of time that must pass without an SGSN response before the GGSN service retransmits GTP control packets.
retransmit_time is measured in seconds and can be configured to an integer from 1 through 20.

Usage

This command is used in conjunction with the **max-retransmissions** command to control the retransmission of GTP control packets when no response is received from an SGSN.
If no response is received from the SGSN prior to the expiration of the timeout value, the GTP control packets are re-sent by the GGSN. This process occurs as many times as allowed by the configuration of the max-retransmissions command.
If the max-retransmissions value is exceeded within the retransmission-timeout period, the GGSN records a "Path Failure" for that SGSN and releases all PDP contexts associated with it.

Important: This retransmission timeout configuration in not applicable for Echo Requests message retransmission. Echo are sent/retransmitted every echo interval, which can be configured separately.

Example

The following command configures a timeout value of *20* seconds:

```
retransmission-timeout 20
```

setup-timeout

Configures the maximum amount of time the GGSN service allows for the setting up of PDP contexts.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

setup-timeout *setup_time*

default setup-timeout

default

Configures the default maximum amount of time the GGSN service allows for the setting up of PDP contexts.

setup-time

Default: 60
Specifies the maximum amount of time the GGSN service allows for the setting up of PDP contexts. *setup_time* is measured in seconds and can be configured to an integer from 1 through 6000.

Usage

Use this command to limit the amount of time allowed for setting up PDP contexts. If the PDP context is not setup within the configured time frame, the GGSN service rejects the PDP context with a cause code of 199 (C7H, No resources available).

Example

The following command allows a maximum of *120* seconds for the setting up of PDP contexts:

```
setup-timeout 120
```

sgsn address

Configures the SGSNs that this GGSN service is allowed to communicate with.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

sgsn address { { *ip_address* [**subnetmask** *netmask*] } | *ip_address/netmask* } [**plmn-foreign** [**reject-foreign-subscriber**] | **mcc** *mcc_code* **mnc** *mnc_code* [**reject-foreign-subscriber**]] [**rat-type** { **GAN** | **GERAN** | **HSPA** | **UTRAN** | **WLAN** }] [**description** *description*] [**disable-gtpc-echo**]

no sgsn { **address** *ip_address* [**subnetmask** *netmask*] }

no

Removes a specific SGSN from the list or all configured SGSNs.

address

Configures the IP address of the SGSN.
ip_address must be expressed in IPv4 dotted-decimal notation.

subnetmask

Configures the subnet mask of the SGSN.
netmask must be expressed in IPv4 dotted-decimal notation.

disable-gtpc-echo

Default: Send GTPC Echo messages to unlisted SGSNs.
When this keyword is specified, GTPC echo messages are not sent to unlisted SGSNs.

plmn-foreign

Indicates whether or not the SGSN belongs to a foreign public land mobile network (PLMN).

reject-foreign-subscriber

Default: Disabled
Specifies that incoming calls from foreign subscribers are rejected.

mcc *mcc_code*

Specifies the mobile country code (MCC) portion of the PLMN's identifier.
mcc_code is the PLMN MCC identifier and configured as an integer from 100 through 999.

mnc *mnc_code*

Specifies the mobile network code (MNC) portion of the PLMN's identifier.
mnc_code is the PLMN MNC identifier and configured as a 2- or 3-digit integer from 00 through 999.

rat-type {GAN | GERAN | HSPA | UTRAN | WLAN }

This keyword configures the type of radio access technology.
GAN: Specifies the Generic Access Network type of Radio Access Technology (RAT).
GERAN: Specifies the GSM EDGE Radio Access Network type of RAT.
HSPA: Specifies the High Speed Packet Access type of RAT.
UTRAN: Specifies the UMTS Terrestrial Radio Access Network type of RAT.
WLAN: Specifies the Wireless Local Access Network type of RAT.

description *description*

Add description field to the SGSN entry in GGSN service.
description is an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure a list of SGSNs that the GGSN service is to communicate with. This command can be entered multiple times to configure multiple SGSNs.

Important: The GGSN only communicates with the SGSNs configured using this command unless a plmn-policy is enabled to allow communication with unconfigured SGSNs. PLMN policies are configured using the **plmn unlisted-sgsn** command.

Example

The following command configures the GGSN to communicate with an SGSN on a foreign PLMN with an IP address of *192.168.1.100* and subnet mask of *255.255.255.0*:

```
sgsn address 192.168.1.100 subnetmask 255.255.255.0 plmn-foreign
```

sgsn define-multiple-address-group

This command defines an SGSN Multiple Address Group and enters SGSN Multiple Address Group Configuration mode. Whenever there is a change in the control address in a GTPC UPC message, it is treated as an inter-SGSN handoff because an SGSN is usually identified uniquely by a single IP-address. This command supports a multiple address group feature which allows you to specify a set of addresses that specify a single SGSN. When a UPC handoff is received from any address in the group, it is treated as an intra-SGSN handoff.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

sgsn define-multiple-address-group *grp_name* **-noconfirm**

no sgsn define-multiple-address-group *grp_name*

no

Removes a specific SGSN Multiple Address Group from the list GGSN service configuration.

grp_name

Specifies the name of an SGSN multiple address group to create or configure.
*grp_name*is an alphanumeric string from 1 through 63 characters.

-noconfirm

Specifies that the command must execute without any additional prompt and confirmation from the user.

Usage

Use this command to create or configure an SGSN Multiple Address Group that the GGSN service is to communicate with. This command can be entered multiple times to configure multiple SGSN Multiple Address Groups.

Example

The following command creates an SGSN Multiple Address Group named *sgsngrp1* and enters SGSN Multiple Address Group Configuration mode:

```
sgsn define-multiple-address-group sgsngrp1
```

sgsn multiple-address-group

Configures the SGSN multiple address groups that this GGSN service is allowed to communicate with.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

sgsn multiple-address-group *grp_name* [**disable-gtpc-echo**] [**mcc** *mcc_code* **mnc** *mnc_code* [**reject-foreign-subscriber**]] [**plmn-foreign** [**reject-foreign-subscriber**] [**rat-type** { **GAN** | **GERAN** | **HSPA** | **UTRAN** | **WLAN** }] [**description** *description*]

no sgsn multiple-address-group *grp_name*

no

Removes a specific SGSN multiple address group from the list of configured SGSN multiple address groups.

grp_name

Specifies the name of a configured SGSN multiple address group to use.

disable-gtpc-echo

Default: Send GTPC Echo messages to unlisted SGSNs.
When this keyword is specified, GTPC echo messages are not sent to unlisted SGSNs.

plmn-foreign

Indicates whether or not the SGSN multiple address group belongs to a foreign public land mobile network (PLMN).

reject-foreign-subscriber

Default: Disabled
Specifies that incoming calls from foreign subscribers are rejected.

mcc *mcc_code*

Specifies the mobile country code (MCC) portion of the PLMN's identifier.
mcc_code is the PLMN MCC identifier and can be configured to an integer from 100 through 999.

mnc *mnc_code*

Specifies the mobile network code (MNC) portion of the PLMN's identifier.
mnc_code is the PLMN MNC identifier configured as a 2- or 3-digit integer from 00 through 999.

rat-type { GAN | GERAN | HSPA | UTRAN | WLAN }

This keyword configures the type of radio access technology.
GAN: Specifies the Generic Access Network type of Radio Access Technology (RAT).
GERAN: Specifies the GSM EDGE Radio Access Network type of RAT.

HSPA: Specifies the High Speed Packet Access type of RAT.
UTRAN: Specifies the UMTS Terrestrial Radio Access Network type of RAT.
WLAN: Specifies the Wireless Local Access Network type of RAT.

description *description*

Add a description field to the SGSN multiple address group entry in the GGSN service configuration. *description* must be an alphameric string of 1 through 63 characters.

Usage

Use this command to configure a list of SGSN multiple address groups with which the GGSN service is to communicate. This command can be entered multiple times to configure multiple SGSN multiple address groups.

Important: The GGSN only communicates with the SGSN multiple address groups configured using this command unless a plmn-policy is enabled to allow communication with unconfigured SGSNs. PLMN policies are configured using the **plmn unlisted-sgsn** command.

Example

The following command configures the GGSN to communicate with an SGSN with multiple address that is defined by an SGSN multiple address group named *sgsngrp1* that is on a foreign PLMN:

```
sgsn multiple-address-group sgsngrp1 plmn-foreign
```

sgsn mcc-mnc

This command configures sgsn mcc-mnc for this GGSN service.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
sgsn mcc-mnc { prefer-rai | prefer-uli }

default sgsn mcc-mnc
```

default

Configures the default option for sgsn mcc-mnc. Default is ‘prefer-uli’.

prefer-rai

Configures sgsn mcc-mnc using rai.

prefer-uli

Configures sgsn mcc-mnc using uli.

Usage

Use this command to configure the sgsn mcc-mnc.

Example

The following command configures the sgsn mcc-mnc to ‘prefer-rai’:

```
sgsn mcc-mnc prefer-rai
```

trace-collection-entity

This command configures the trace collection entity IP address. Trace collection entity is the destination node to which trace files are transferred and stored.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

trace-collection-entity *IPv4_addr*

no trace-collection-entity

no

Removes the configured IPv4 address for trace collection in this GGSN service.

IPv4_addr

Specifies the IP address in IPv4 dotted-decimal notation.

Usage

Use this command to configure the trace collection entity IP address. This configuration is required because during signaling session trace activation, CPC REQ and UPC REQ do not provide the IP address for the trace collection entity.

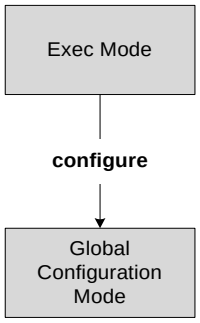
Example

The following command configures the trace collection entity IP address with this GGSN service:

```
trace-collection-entity 192.36.56.56
```

Chapter 127
Global Configuration Mode Commands

The Global Configuration Mode is used to configure basic system-wide parameters.



aaa accounting-overload-protection

This command configures Overload Protection Policy for accounting requests.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
aaa accounting-overload-protection prioritize-gtpp

{ default | no } aaa accounting-overload-protection
```

default

Configures the default setting.
Default: no priority assigned

no

Disables the Overload Protection configuration.

prioritize-gtpp

Gives higher priority to GTPP requests among the other outstanding requests. So while purging the lower priority requests will be selected first.

Usage

Use this command to configure Overload Protection Policy for accounting requests.

Example

The following command prioritizes GTPP requests among the other outstanding requests:

```
aaa accounting-overload-protection prioritize-gtpp
```

aaa default-domain

Configure global accounting and authentication default domain for subscriber and context-level administrative user sessions.

Product

All

Privilege

Security Administrator, Administrator

Syntax

aaa default-domain { administrator | subscriber } *domain_name*

no aaa default-domain { administrator | subscriber }

no

Removes all or only the specified configured domain.

administrator | subscriber

administrator: Configures the default domain for context-level administrative users.
subscriber: Configures the default domain for subscribers.

domain_name

Sets the default context.
domain_name must be an alphanumeric string of 1 through 79 characters.

Usage

This command configures the default domain which is used when accounting and authentication services are required for context-level administrative user and subscriber sessions whose user name does not include a domain.

Example

The following commands configure the default domains for context-level administrative users and subscribers, respectively:

```
aaa default-domain administrator sampleAdministratorDomain

aaa default-domain subscriber sampleSubscriberDomain
```

aaa domain-matching ignore-case

This command disables case sensitivity when performing domain matching. When this command is enabled, the system disregard case when matching domains.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] aaa domain-matching ignore-case

default aaa domain-matching
```

default

Configures ignore-case as the domain matching method.

no

Specifies that the system consider case when domain matching.

Usage

Use this command to configure the system to ignore case when matching domains.

Example

The following command configures the system to ignore case when matching domains:

```
aaa domain-matching ignore-case
```

aaa domain-matching imsi-prefix

Enables domain lookup for session based on the International Mobile Subscriber Identity (IMSI) prefix length. Default: Disabled

Important: This command is only available in 8.3 and later releases.

Product

All

Privilege

Security Administrator, Administrator

Syntax

aaa domain-matching imsi-prefix prefix-length *prefix_length*

no aaa domain-matching imsi-prefix

default aaa domain-matching

no

Specifies the system must not consider imsi-prefix domain matching method.

prefix-length

Specifies the IMSI length to be matched with the domain.
prefix_length must be an integer from 1 through 15.

Usage

Use this command to configure the IMSI-prefix method of domain matching. This command enables domain lookup for the session based on the IMSI prefix length. If there is a domain configured with the matching IMSI prefix, the associated configuration is used.
This feature does not support partial matches.

Example

The following command configures the IMSI prefix method for domain matching setting the prefix length to *10*.

```
aaa domain-matching imsi-prefix prefix-length 10
```

aaa large-configuration

This command enables or disables the system to accept a large number of RADIUS configurations to be defined and stored.

Important: For this command to take affect, after entering the command the configuration must be saved and reloaded.

When aaa large-configuration is disabled, the following restrictions are in place:

- Only one (1) NAS IP address can be defined per context with the **`radius attribute`** command.
- The RADIUS attribute **nas-ip-address** can only be configured if the RADIUS group is **default**.
- Only 320 RADIUS servers can be configured system-wide.
- Only 64 RADIUS groups can be configured system-wide.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] aaa large-configuration
```

`no`

Disables AAA large configuration support.

Usage

When aaa large-configuration is enabled, the system provides the ability to configure multiple NAS IP addresses in a single context to used with different radius groups. As well, the command allows support for up to 1,600 RADIUS server configurations and for a PDSN a maximum of 400 or for a GGSN a maximum of 800 RADIUS server group configurations system-wide.

Example

To enable the definition of a large number of RADIUS configurations, enter the following commands in the following order:
In APN Configuration mode, enter:

```
default aaa group
```

In Global Configuration mode, enter:

```
aaa large-configuration
```

In Exec mode, use the **`save configuration`** command and then the **`reload`** command.

aaa last-resort

Configure global accounting and authentication last resort domain for subscriber and context-level administrative user sessions.

Product

All

Privilege

Security Administrator, Administrator

Syntax

aaa last-resort context { administrator | subscriber *context_name* **}**

no aaa last-resort context { administrator | subscriber }

no

Removes all or only the specified previously configured authentication last resort domain name.

administrator | subscriber

administrator: Configures the last resort domain for context-level administrative.
subscriber: Configures the last resort domain for the subscribers.

context_name

Specifies the context which is to be set as the last resort. *context_name* must be an alphanumeric string of 1 to 79 characters.

Usage

Set the last resort context which is used when there is no applicable default domain (context) and there is no domain provided with the subscriber's or context-level administrative user's name for use in the AAA functions.

Example

The following commands configure the last resort domains for context-level administrative user and subscribers, respectively:

```
aaa last-resort administrator sampleAdministratorDomain

aaa last-resort subscriber sampleSubscriberDomain
```

The following command removes the previously configured domain called *sampleAdministratorDomain*:

```
no aaa last-resort administrator sampleAdministratorDomain
```

aaa tacacs+

This command enables or disables system-wide TACACS+ AAA (authentication, authorization and accounting) services for administrative users. This command is valid only if TACACS+ servers and related services have been configured in TACACS Configuration Mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] aaa tacacs+
```

Usage

Enables or disables the use of TACACS+ AAA services for administrative users.

Example

```
aaa tacacs+

no aaa tacacs+
```

aaa username-format

Configure global accounting and authentication user name formats for AAA (authentication, authorization and accounting) functions. Up to six formats may be configured.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] aaa username-format { domain | username } separator

default aaa username-format
```

no

Removes the specified user name format from the configuration.

domain | username

Default: username @
domain: indicates the left side of the string from the separator character is a domain name and the right side is the user name.
username: indicates the left side of the string from the separator character is a user name and the right side is the domain name.

Important: The user name string is always searched from right to left for the first occurrence of the separator character.

separator

Specifies the character to use to delimit the domain from the user name for global AAA functions.Permitted characters include: @, %, -, \, #, or /. To specify a back slash ('\') as the separator, you must enter a double back slash ('\\') on the command line.

Usage

Define the formats for user name delimiting if certain domains or groups of users are to be authenticated based upon their user name versus domain name.

Example

```
aaa username-format domain @

aaa username-format username %

no aaa username-format username %
```

active-charging service

This command allows you to create/configure/delete the Active Charging Service (ACS)/Enhanced Charging Service (ECS).

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

active-charging service *acs_service_name* **[-noconfirm]**

no active-charging service *acs_service_name*

no

Deletes the specified Active Charging Service.

acs_service_name

Specifies name of the Active Charging Service.
acs_service_name must be the name of an Active Charging Service, and must be an alphanumeric string of 1 through 15 characters.
If the named Active Charging Service does not exist, it is created, and the CLI mode changes to the ACS Configuration Mode wherein the service can be configured. If the named Active Charging Service already exists, the CLI mode changes to the ACS Configuration Mode.

-noconfirm

Specifies that the command must execute without any additional prompt and confirmation from the user.

Usage

Use this command to create/configure/delete an Active Charging Service in the system. Note that, in this release, only one Active Charging Service can be created in the system.
Use this command after enabling ACS using the **require active-charging** command. This command allows administrative users to configure the ACS functionality.

Example

The following command creates an ACS service named *test*:

```
active-charging service test
```

alarm

Enables or disables alarming options for the SPIO card internal alarms and the central-office external alarms. To verify the state of the alarms, refer to the **show alarm** command.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
alarm { audible | central-office  }

no alarm { audible | central-office  }
```

no

Disables the option specified.

audible | central-office

audible: indicates the internal audible alarm on the SPIO cards are to be enabled.
central-office: indicates the central office alarms are to be enabled.

Usage

Disable CO and audible alarms when an existing device provides such capability.

Example

The following commands enable the SPIO card internal alarms and disable the central office alarms, respectively.

```
alarm audible

no alarm central-office
```

apn-profile

Creates an instance of an Access Point Name (APN) profile.

Product

MME, SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] apn-profile *apn_profile_name*

no

Deletes the APN profile instance from the configuration.

apn_profile_name

Specifies the name of the APN profile. Enter an alphanumeric string of 1 through 64 characters.

Usage

Use this command to create an instance of an APN profile and to enter the APN profile configuration mode. An APN profile is a template which groups a set of APN-specific commands that may be applicable to one or more APNs. See the *APN Profile Configuration Mode Commands* chapter for information regarding the definition of the rules contained within the profile and the use of the profile.

Important: An APN profile is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what APN profiles have already been created, return to the Exec mode and enter the **show apn-profile all** command.

Example

The following command creates a configuration instance of an APN profile:

```
apn-profile apnprof27
```

apn-remap-table

Creates an instance of an Access Point Name (APN) remap table.

Product

MME, SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] apn-remap-table *apn_remap_table_name*

no

Deletes the APN remap table instance from the configuration.

apn_remap_table_name

Specifies the name of the APN remap table. Enter an alphanumeric string of 1 through 65 characters.

Usage

Use this command to create an instance of an APN remap table and to enter the APN remap table configuration mode. An APN remap table includes entries that define how an incoming APN, or the lack on one, will be handled. See the *APN Remap Table Configuration Mode Commands* chapter for information regarding the definition of the entries contained within the table and the use of the table.

Important: An APN remap table is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what APN remap tables have already been created, return to the Exec mode and enter the **show apn-remap-table all** command.

Example

The following command creates a configuration instance of an APN remap table:

```
apn-remap-table pnremap-USorigins-table1
```

arp

Configures a system-wide time interval for performing Address Resolution Protocol (ARP) refresh.

Product

All

Privilege

Security Administrator, Administrator

Syntax

arp base-reachable-time *time*

default arp base-reachable-time

default

Restores the parameter to its default setting.

time

Default: 30
Specifies the ARP refresh interval (in seconds) as an integer from 30 through 86400.

Usage

Use this command to configure a system-wide ARP refresh interval. Once a neighbor is found, the entry is considered valid for at least a random value between the *time*/2 and the *time**1.5.

Example

The following command configures an ARP refresh interval of 1 hour:

```
arp base-reachable-time 3600
```

autoconfirm

This command disables or enables confirmation for certain commands. This command affects all future CLI sessions.

Important: To change the behavior for the current CLI session only, use the **autoconfirm** command in the Exec Mode.

Product

All

Privilege

Security Administrator, Administrator, Operator

Syntax

autoconfirm

no autoconfirm

Usage

When autoconfirm is enabled, certain commands ask you to answer yes or no to confirm that you want to execute the command. When autoconfirm is disabled the confirmation questions never appear. Disabling autoconfirm disables command confirmation for all future CLI sessions.
By default **autoconfirm** is enabled.

Example

The following command enables command confirmation for all future CLI sessions;

```
autoconfirm
```

The following command disables command confirmation for all future CLI sessions;

```
no autoconfirm
```

autoless

This command is obsolete. It is included in the CLI for backward compatibility with older configuration files. When executed, this command issues a warning and performs no function.

banner

Configures the CLI banner which is displayed upon the start of a CLI session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

banner { charging-service | lawful-intercept | motd | pre-login } *string*

no banner { charging-service | lawful-intercept | motd | pre-login }

no

Removes the banner message by setting it to be a string of zero length.

charging-service

Specifies the Active Charging Service banner message. The banner is displayed upon initialization of an SSH CLI session with ACS-admin privileges (whenever anyone with the CLI privilege bit for ACS logs on).

lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

motd

Configures the CLI banner message of the day which is displayed upon the initialization of any CLI session.

pre-login

Configures the CLI banner displayed before a CLI user logs in.

Important: This banner is displayed only for serial port and telnet log ins. It is not supported in ssh and, therefore, will not be displayed before ssh log ins.

string

Specifies the banner or message to be displayed at session initialization. *string* may be an alphanumeric string of 0 through 2048 characters. The string must be enclosed in double quotation marks if the banner or message is to include spaces.

Usage

Set the message of the day banner when an important system wide message is needed. For example, in preparation for removing a chassis from service, set the banner 1 or more days in advance to notify administrative users of the pending maintenance.

Example

```
banner motd "Have a nice day."
```

```
banner motd No_News_Today

no banner motd
```

boot delay

Configures the delay period, in seconds, before attempting to boot the system from a software image file residing on an external network server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

boot delay *time*

no boot delay

no

Deletes the setting for the boot delay. The boot process executes immediately.

time

Specifies the amount of time (in seconds) to delay prior to requesting the software image from the external network server as an integer from 1 through 300.

Usage

Useful when booting from the network when connection delays may cause timeouts. Such as when the Spanning Tree Protocol is used on network equipment.

Important: The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

Example

The following sets the boot delay to *10* seconds:

```
boot delay 10
```

boot interface

Configures the Switch Processor I/O card network interfaces for obtaining a system software image during the system boot process.

Product

All

Privilege

Security Administrator, Administrator

Syntax

boot interface { spio-eth1 | spio-eth2 } [medium { auto | speed *medium_speed* **duplex** *medium_duplex* **} [media** *medium_media* **]]**

no boot interface

---

no

Removes the boot interface configuration from the boot.sys file. Only files from the local file system can be loaded.

---

spio-eth1 | spio-eth2

Specifies the network interface to be configured where **spio-eth1** is the primary interface on the SPIO (slot 24 interface 1 or slot 25 interface 1) and **spio-eth2** is the secondary interface on the SPIO (slot 24 interface 2 or slot 25 interface 2). The interfaces refer to either the RJ-45 interfaces for speeds of 10, 100, or 1000 megabit per second (Mbps), or the SFP interface for the optical gigabit (1000 Mbps) interface.

---

medium { auto | speed *medium_speed* **duplex** *medium_duplex* **}**

Default: auto
auto: configures the interface to auto-negotiate the interface speed. and duplex.
speed *medium_speed* **duplex** *medium_duplex*: specifies the speed to use at all times where *medium_speed* must be one of:

- 10
- 100
- 1000

The keyword **duplex** is used to set the communication mode of the interface where *medium_duplex* must be one of:

- full
- half

---

media *medium_media*

Default: rj45
Optionally sets the physical interface where *medium_media* must be either rj45 or sfp.

Usage

Modify the boot interface settings to ensure the system is able to obtain a software image from an external network server.

Important: The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

Example

The following configures the primary interface to auto-negotiate the speed.

```
boot interface spio-eth1 medium auto
```

The following command configures the secondary interface to a fixed gigabit speed at full duplex using RJ45 connectors for the physical interface.

```
boot interface spio-eth2 medium speed 1000 duplex full media rj45
```

The following restores the defaults for the boot interface.

```
no boot interface
```

boot nameserver

Configures the IP address of the DNS (Domain Name Service) server to use when looking up hostnames in URLs for network booting.

Product

All

Privilege

Security Administrator, Administrator

Syntax

boot nameserver *ip_address*

no boot nameserver

ip_address

IPv4 dotted-decimal address of the DNS server the system uses to lookup hostnames in URLs for a software image from the network during the system boot process.

no

Removes the network boot nameserver information from the boot.sys file.

Usage

Use this command to identify the DNS server to use to lookup hostnames in a software image URL.

Important: The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

Example

The following configures the system to communicate with a DNS nameserver with the IP address of 10.2.3.4:

```
boot nameserver 10.2.3.4
```

boot system priority

Specifies the priority of a boot stack entry to use when the system first initializes or restarts. Up to 10 boot system priorities (entries in the boot.sys file located in the /flash device in the SMC) can be configured.

Product

All

Privilege

Security Administrator, Administrator

Syntax

boot system priority *number* **image** *image_url* **config** *config_path*

no boot system priority *number*

no

Remove a boot stack entry at the priority specified from the boot stack when it is no longer used.

priority *number*

Specifies the priority for the file group (consisting of an image (.bin) and its corresponding configuration (.cfg) file) specified in the boot stack. The value must be in the range from 1 through 100 where a priority of 1 is the highest. Up to 10 boot system priorities (boot stack entries) can be configured.

Important: When performing a software upgrade it is important that the new file group have the highest priority (lowest value) configured.

Important: To ensure that higher priority numbers remain open, use an "N-1" priority numbering methodology, where "N" is the first priority in the current boot stack.

image *image_url*

Specifies the location of a image file to use for system startup. The URL may refer to a local or a remote file. The URL must be formatted according to the following format:

- [**file:**]{ **/flash** | **/pcmcia1** | **/hd** }[**/***directory*]**/***filename*
- [**http:** | **tftp:**]**//***host*[**:***port*][**/***directory*]**/***filename*

Important: Use of the SMC hard drive is not supported in this release.

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.

filename is the actual file of interest.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

Important: A file intended for use on an ASR 5000 uses the convention xxxxx.asr5000.bin, where xxxxx is the software build number.

Important: When using the TFTP, it is advisable to use a server that supports large blocks, per RFC 2348. This can be implemented by using the "block size option" to ensure that the TFTP service does not restrict the file size of the transfer to 32MB.

config *config_path*

Specifies the location of a configuration file to use for system startup. This must be formatted according to the following format:

- [**file:**]{ **/flash** | **/pcmcia1** | **/pcmcia2** }[**/***path*]**/***filename*
- ASR 5000:
- [**file:**]{ **/flash** | **/pcmcia1** | **/hd** }[**/***path*]**/***filename*

Important: Use of the SMC hard drive is not supported in this release.

Where *path* is the directory structure to the file of interest, and *filename* is the name of the configuration file. This file typically has a **.cfg** extension.

Usage

This command is useful in prioritizing boot stack entries in the boot.sys file, typically located on the /flash device of the Active SMC, for automatic recovery in case of a failure of a primary boot file group.

Important: The configuration file must reside on the local filesystem, stored on one of its local devices (/flash, /pcmcia1, /hd-raid). Attempts to load the configuration file from an external network server will result in a failure to load that image and configuration file group, causing the system to load the image and configuration file group with the next highest priority in the boot stack.

Important: Configuration changes do not take effect until the system is reloaded.

Important: The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

Example

The following commands set up two locations to obtain a boot file group from.

```
boot system priority 1 image tftp: //remoteABC/pub/2012jan.bin config
/flash/pub/data/2012feb.cfg
```

```
boot system priority 2 image /flash /pub/data/2002jun.bin config
/pcmcia1/pub/data/2012feb.cfg
```

The following removes the current priority **1** boot entry from the boot.sys file.

```
no boot system priority 1
```

bulkstats

Enables the collection of bulk statistics by the system and/or enters the bulk statistic configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
bulkstats { collection | historical | mode }

no bulkstats collection
```

collection

Enables the statistics collection process. Collects a period snapshot of data, such as “here is what the value is right now”.

historical collection

Enables the system to collect historical bulk statistics.
If enabled, the system keeps track of some things which require the storing of more data, such as “the highest value that’s been seen over the last 24 hours”.

mode

Enters the bulk statistics configuration mode. The resulting command-line prompt will look similar to:

```
[<context-name>]asr5000(config-bulkstats)#
```

no

Disables the collection of bulk statistics.

Usage

The Bulk Statistics Configuration Code consists of commands for configuring bulk statistic properties, such as the period of collection. Bulk Statistics configuration mode commands are defined in the *Bulk Statistics Configuration Mode Commands* chapter.
The system can be configured to collect bulk statistics and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group or schema, for example, system statistics, port statistics, radius statistics.
Once bulk statistics receiver, schema, and collection properties are configured, this **bulkstats** command is used to enable or disable the collection of the data.
To collect a sample that will provide an average, for example, an average of CPU counters, the “historical” features must be enabled with the **bulkstats historical collection** command.
Since bulk statistics are collected at regular, user-defined intervals, the **bulkstats force** command in the Exec Mode can be used to manually initiate the collection of statistics at any time.

Example

```
bulkstats collection
```

bulkstats mode

no bulkstats collection

ca-certificate

Configures and selects an X.509 CA root certificate to enable a security gateway or SCM to perform certificate-based peer (client) authentication. The system supports a maximum of 16 certificates and 16 CA root certificates. A maximum of four CA root certificates can be bound to a crypto or ssl template.

Product

FNG, SCM (P-CSCF, A-BG)

Privilege

Administrator, Security Administrator, Operator

Syntax

ca-certificate name *name* **pem { data** *pemdata* **| url** *url* **}**

no ca-certificate name *name*

name *name*

Names the CA certificate. *name* must be an alphanumeric string of 1 through 128 characters.

pem

Specifies that the Privacy-enhanced Electronic Mail (PEM) format is to be used.

data *pemdata*

CA certificate data in PEM format. *pemdata* must be an alphanumeric string of 1 through 4095 characters.

url *url*

URL of the file containing CA certificate in PEM. *url* must be an existing URL expressed in one of the following formats:

- `[file:]{/flash | /pcmcia1 | /hd-raid}[/directory]/<filename`
- `tftp://<host>[:<port>][/<directory>]/<filename`
- `ftp://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename`
- `sftp://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename`
- `http://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename`

When read via a file, note that **show configuration** will not contain the URL reference, but will instead output the data via **data pemdata**, such that the configuration file is self-contained.

no

Removes the named CA certificate.

Usage

In addition to the X.509 certificate-based gateway authentication method and the PSK (Pre-Shared Key) and EAP-AKA (Extensible Authentication Protocol - Authentication and Key Agreement) peer (client) authentication methods, the FNG and SCM support X.509 certificate-based peer authentication.

The FNG checks the network policy on whether a FAP is authorized to provide service. If the network policy states that all FAPs that pass device authentication are authorized to provide service, no further authorization check may be required. If the network policy requires that each FAP be individually authorized for service (in the case where the FEID is associated with a valid subscription), the FNG sends a RADIUS Access-Request message to the AAA server. If the AAA server sends a RADIUS Access-Accept message, the FNG proceeds with device authentication. Otherwise, the FNG terminates the IPSec tunnel setup by sending an IKEv2 Notification message indicating authentication failure.
The operator/administrator is responsible for configuring the certificates through the CLI. The system will generate an SNMP notification when the certificate is within 30 days of expiration, and then once a day.

Example

Use the following command to remove a certificate named *fap1*:

```
no ca-certificate data fap1
```

ca-crl

Configures the name and URL path of a Certificate Authority-Certificate Revocation List (CA-CRL).

Product

S-GW

PDG/TTG

PDIF

FNG

HNB-GW

SCM (P-CSCF, A-BG)

Privilege

Operator

Syntax

ca-crl name *name* **{ der | pem } { url** *url* **}**

no ca-crl name *name*

no

Removes the named CA-CRL.

name

Provides a name of the CA-CRL. *name* must be an alphanumeric string of 1 through 128 characters.

der

Specifies that the Distinguished Encoding Rules (DER) format is to be used for the source format.

pem

Specifies that the Privacy-enhanced Electronic Mail (PEM) format is to be used for the source format.

url *url*

Specifies the URL where the CA-CRL is to be fetched. *url* must be an existing URL expressed in one of the following formats:

- `[file:]{/flash | /pcmcia1 | /hd-raid}[/directory]/<filename`
- `tftp://<host>[:<port>][/<directory>]/<filename`
- `ftp://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename`
- `sftp://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename`
- `http://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename`

Usage

Use this command to name and fetch a CA-CRL from a specified location.

Without additional information from the CA, an issued certificate remains valid to any verifier until it expires. To revoke certificates, the CA publishes a CRL periodically to provide an updated list of certificates revoked, but not yet expired. Like a certificate, a CRL is a digital document signed by the CA. In addition to a list of serial numbers of revoked certificates, the CRL includes attributes such as issuer name (same as the issuer name in the certificate), signature (signed by the issuer using the same key that signs certificates), last update (the time this CRL was issued), and next update (the time next CRL will be available).

Example

The following command fetches a CA-CRL named *list1.pem* from a *host.com/CRLs* location and names the list *CRL5*:

```
ca-crl name CRL5 pem url http://host.com/CRLs/list1.pem
```

card

Enters the card configuration mode for the card specified.

Product

All

Privilege

Security Administrator, Administrator

Syntax

card *number*

number

Specifies the number of the card for which the card configuration mode is to be entered. *number* must be an integer from 1 through 48.

Usage

Enter the configuration mode for a specific card when changes a required.

Important: This command is not supported on all platforms.

Example

```
card 8
```

card-standby-priority

Configures the redundancy priorities for packet processing cards by specifying the slot number search order for a standby card when needed.

Product

All

Privilege

Security Administrator, Administrator

Syntax

card-standby-priority *slot_num* **[** *slot_num* **]** **[** *slot_num* **]** **...**

slot_num

Specifies the slot of the card for the order of the standby cards. *slot_num* must be in the range from 1 through 16 excluding slots 8 and 9. *slot_num* may be repeated as many times as necessary to indicate the complete search order.

Usage

Set the standby order of the redundant cards when multiple standby cards are available. Questionable hardware should be placed lower in the priority list.

Important: This command replaces the **pac-standby-priority** command.

Important: This command is not supported on all platforms.

Example

The following command configures the redundancy priority to use the standby cards in slots 16, 14, and 12 in that order:

```
card-standby-priority 16 14 12
```

call-control-profile

Creates an instance of a call-control profile.

Product

MME, SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] call-control-profile *cc_profile_name*

no

Deletes the Call-Control Profile instance from the configuration.

cc_profile_name

Specifies the name of the call-control profile. Enter an alphanumeric string of 1 through 64 characters.

Usage

Use this command to create an instance of a call-control profile and to enter the call-control profile configuration mode. A call-control profile is a template which groups a set of call-handling instructions that may be applicable to one or more incoming calls. See the *Call-Control Profile Configuration Mode Commands* chapter for information regarding the definition of the rules contained within the profile and the use of the profile.

Important: A call-control profile is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what call-control profiles have already been created, return to the Exec mode and enter the **show call-control-profile all** command.

Example

The following command creates a configuration instance of an call-control profile:

```
call-control-profile ccprof1
```

cdr-multi-mode

This command enables multiple instances of CDRMOD, one per packet processing card.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
[ default ] cdr-multi-mode
```

default

Configures this command with its default setting.
Default: Single-CDRMOD mode

Usage

Use this command to enable the multi-CDRMOD mode, wherein there will be one instance of CDRMOD per packet processing card. All the SessMgr instances that are running on a packet processing card will send the records to the CDRMOD instance running on that card.
By default, CDRMOD runs in single mode, wherein there will be only one instance of CDRMOD running for the entire chassis. All the SessMgr instances that are running on a packet processing card will send the records to the CDRMOD instance.

Important: For changes to this command to take effect, save the configuration and reboot the system.

Important: In multi-CDRMOD mode, you should enable hard-disk usage.

certificate

Configures and selects an X.509 Trusted Author certificate.

Product

ACS

FNG

PDG/TTG

PDIF

SCM (P-CSCF, A-BG)

Privilege

Administrator, Security Administrator, Operator

Syntax

certificate name *name* **pem { data** *pemdata* **| url** *url* **} private-key pem { [encrypted] data** *pemdata* **| url** *url* **}**

no certificate name *name*

---

name *name*

Names the certificate. *name* must be from 1 to 128 alphanumeric characters.

---

pem

Specifies that the Privacy-enhanced Electronic Mail (PEM) format is to be used.

---

data *pemdata*

Certificate/private key data in PEM format. *pemdata* must be an alphanumeric string of 1 through 4095 (certificate) or 1 through 8191 (private key) characters.

---

url *url*

URL of the file containing certificate/private key in PEM. *url* must be an existing URL expressed in one of the following formats:

- `[file:]{/flash | /pcmcia1 | /hd-raid}[/directory]/<filename`
- `tftp://<host>[:<port>][/<directory>]/<filename`
- `ftp://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename`
- `sftp://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename`
- `http://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename`

When read via a file, **show configuration** will not contain the URL reference, but instead outputs the data via **data** *pemdata*, such that the configuration file is self-contained.

---

private-key

Private key data.

encrypted

Encrypted private key data.

no

Removes the named certificate.

Usage

A certificate authority or certification authority (CA) is an entity which issues digital certificates for use by other parties. It is an example of a trusted third party. CAs are characteristic of many public key infrastructure (PKI) schemes.
If CERT information is configured, the system will include the CERT payload in the first IKE_AUTH Response during the first authentication. The system stores its own certificate for use in the first AUTH calculation. MS will not have its own certificate from CA. Still, it will be capable of accepting a certificate from the system and verify AUTH.
The operator/administrator is responsible for configuring the certificates through the CLI. The system will generate an SNMP notification when the certificate is within 30 days of expiration, and then once a day.

Example

Use the following command to remove a certificate named *box1*:

```
no certificate data box1
```

cli

Configures global Command Line Interface (CLI) parameters.

Product

All

Privilege

Security Administrator, Administrator

Syntax

cli { access { monitor-protocol | monitor-subscriber | show-configuration } { administrator | operator } } | login-failure-delay *number* **| max-sessions** *number* **| operator clear-subscriber-one-only | trap config-mode }**

no cli { max-sessions | login-failure-delay *number* **| operator clear-subscriber-one-only | trap config-mode }**

default cli { access { monitor-protocol | monitor-subscriber | show-configuration } | max-sessions | login-failure-delay *number* **| operator clear-subscriber-one-only | trap config-mode }**

no

Removes the limit on the number of allowed simultaneous CLI sessions on the system. or removes the limit of how many subscribers an Operator can clear.

default

Resets the keywords to their default values.

access { monitor-protocol | monitor-subscriber | show-configuration } { operator | administrator }

Sets access privileges on the **monitor protocol** and **monitor subscriber** commands:
monitor-protocol: Selects privileges for the **monitor protocol** command.
monitor-subscriber: Selects privileges for the **monitor subscriber** command.
show-configuration: Selects privileges for the **show-configuration**command. However the default access level for this command is the user with operator privileges.
operator: Sets the privileges for the selected command to allow use by users with operator privileges.
administrator: Restricts use of the selected command to administrators only.

login-failure-delay *number*

This is the time to wait before a login failure is returned and another login may be attempted. Default is five seconds.

max-sessions *number*

Sets the number of allowed simultaneous CLI sessions on the system. If this value is set to a number below the current number of open CLI sessions, the open sessions will continue until closed. *number* must be an integer from 2 through 100.

Caution: Use caution when setting this command. Limiting simultaneous CLI sessions prevents authorized users from accessing the system if the maximum number allowed has been reached. The system already limits CLI sessions based on available resources. Additional limitation could have adverse effects.

operator clear-subscriber-one-only

Restricts Operator to clearing only one subscriber session at a time.

trap config-mode

Enables sending an SNMP notification (trap) when a CLI user enters the configuration mode.

Usage

This command limits the number of simultaneous CLI sessions on the system at any given time.

Example

The following command sets the number of allowed simultaneous CLI sessions to 5.

```
cli max-sessions 5
```

The following command sets the command **monitor protocol** to administrator-only

```
cli access monitor-protocol administrator
```

clock

Configures system clock timezone and what local time zone to use.

Product

All

Privilege

Security Administrator, Administrator

Syntax

clock timezone *tz* **[local]**

no clock timezone

no

Resets the system timezone to the system default UTC.

tz

Specifies the system time zone to use as one of:

- america-buenos-aires (GMT-3:00; Buenos Aires)
- america-caracas (GMT-4:00) Caracas
- america-guatemala (GMT-6:00; Guatemala, Guatemala)
- america-la_paz (GMT-4:00; La Paz)
- america-lima (GMT-5:00; Lima, Peru)
- america-puerto-rico (GMT-4:00; Puerto Rico)
- america-sao-paulo (GMT -3:00; Brazil)
- america-tijuana (GMT-8:00; Tijuana)
- asia-baghdad (GMT+3:00; Baghdad, Russia Zone 2, Kuwait, Nairobi, Riyadh, Moscow, Tehran)
- asia-bangkok (GMT+7:00; Bangkok)
- asia-calcutta (GMT+5:30; Calcutta, Mumbai, New Delhi)
- asia-dhaka (GMT+6:00; Dhaka)
- asia-hong-kong (GMT+8:00; Hong_Kong)
- asia-irkutsk (GMT+9:30; Irkutsk)
- asia-kabul (GMT+4:30; Kabul)
- asia-karachi (GMT+5:00; Karachi)
- asia-katmandu (GMT+5:45; Kathmandu)
- asia-magadan (GMT+11:00; Magadan)
- asia-muscat (GMT+4:00; Abu Dhabi, UAE, Muscat, Tblisi, Volgograd, Kabul)
- asia-rangoon (GMT+6:30; Rangoon)
- asia-seoul (GMT+9:00) Seoul
- asia-tehran (GMT+3:30; Tehran)

- asia-tokyo (GMT+9:00; Tokyo, Russia Zone 8)
- atlantic-azores (GMT-2:00; Azores)
- atlantic-cape-verde (GMT-1:00; Cape Verde Islands)
- australia-perth (GMT+8:00) Perth
- australia-darwin (GMT+9:30) Northern Territory - Alice Springs, Darwin, Uluru
- australia-adelaide (GMT+9:30) Southern Territory - Adelaide
- australia-melbourne (GMT+10:00) Victoria - Ballarat, Melbourne
- australia-sydney (GMT+10:00) New South Wales - Newcastle, Sydney, Wollongong
- australia-hobart (GMT+10:00) Tasmania - Hobart, Launceston
- australia-brisbane (GMT+10:00) Queensland - Brisbane, Cairns, Toowoomba, Townsville
- australia-lordhowe (GMT+10:30) Lord Howe Island
- canada-newfoundland (GMT-3:30; Newfoundland)
- canada-saskatchewan (GMT-6:00; Saskatchewan)
- europe-central (GMT+1:00; Paris, Berlin, Amsterdam, Brussels, Vienna, Madrid, Rome, Bern, Stockholm, Oslo)
- europe-dublin (GMT+0:00) Dublin, Ireland
- europe-eastern (GMT+2:00; Russia Zone 1, Athens, Helsinki, Istanbul, Jerusalem, Harare)
- newzealand-auckland (GMT +12:00; Auckland, Willington)
- newzealand-chatham (GMT +12:45; Chatham)
- nuku (GMT-13:00; Nuku'alofa)
- pacific-fiji (GMT+12:00; Wellington, Fiji, Marshall Islands)
- pacific-guam (GMT+10:00; Brisbane, Cairns, Sydney, Guam)
- pacific-kwajalein (GMT-12:00; Kwajalein)
- pacific-norfolk - (GMT+11:30) Norfolk Island
- pacific-samoa (GMT-11:00; Samoa)
- us-alaska (GMT-9:00; Alaska)
- us-arizona (GMT-7:00; Arizona)
- us-central (GMT-6:00; Chicago, Mexico City, Saint Louis)
- us-eastern (GMT-5:00; Bogota, Lima, New York City)
- us-hawaii (GMT-10:00; Hawaii)
- us-indiana (GMT-6:00; Indiana)
- us-mountain (GMT-7:00; Cheyenne, Denver, Las Vegas)
- us-pacific (GMT-8:00) San Francisco, LA, Seattle
- utc (GMT; Universal Time Coordinated: London, Dublin, Edinburgh, Lisbon, Reykjavik, Casablanca)

`local`

Indicates the timezone specified by *`tz`* is to be considered the local time zone for local time display and conversion.

Usage

Clock and timezone management is necessary for proper accounting records. The chassis may be set to display a different local time than that of the system clock which allows accounting records to use the system time but to display the proper local time for users.

Example

```
clock timezone utc

clock timezone us-indiana local

no clock timezone
```

congestion-control

Enables or disables support for congestion control on the system.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
congestion-control policy

default congestion-control

no congestion-control
```

default

Sets the congestion control to its default value.

no

Disables congestion control functionality. This is the default setting.

Usage

Congestion control on the system is used to monitor the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (i.e high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may impact the system's ability to service subscriber sessions. The purpose of congestion control is to aid in the identification of such conditions and invoke policies for addressing the situation.

Congestion control operation is based on the configuration of the following:

- **Congestion condition thresholds:** Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). These thresholds function in a similar fashion to the operation thresholds that can be configured for the system (as described in later in this chapter). The primary difference is that when these thresholds are reached, not only is an SNMP trap generated (starCongestion), but a service congestion policy is invoked as well.

A threshold tolerance is configured to dictate the percentage under the configured threshold that must be reached in order for the condition to be considered "cleared". An SNMP trap (starCongestionClear) is then triggered.

- **Service congestion policies:** Congestion policies are configurable for each service (PDSN, GGSN, or HA). These policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

Because congestion control functionality on the system is disabled by default, this command should be executed once congestion-control thresholds and policies have been configured. (Refer to the **congestion-control policy** and **congestion-control threshold** commands for more information.)

congestion-control overload-disconnect

This command enables and disables the policy for disconnecting passive calls (chassis-wide) during an overload situation. It also configures and fine-tunes the overload-disconnect congestion control policy for an entire chassis.

Product

All

Privilege

Security Administrator, Administrator

Syntax

congestion-control overload-disconnect [iterations-per-stage *integer* **| percent** *percentage_value* **| threshold { license-utilization** *percentage_value* **| max-sessions-per-service-utilization** *percentage_value* **| tolerance** *number* **}]**

default congestion-control overload-disconnect [iterations-per-stage | percent | threshold { license-utilization | max-sessions-per-service-utilization | tolerance }]

no congestion-control overload-disconnect

---

iterations-per-stage *integer*

Specifies the number of calls to be disconnected during the defined number of seconds. *integer* is a value from 2 through 8. The default value is 8.

---

percent *percentage_value*

Specifies the percentage of calls to be disconnected, in stages, during an overload situation. *percentage_value* is an integer from 1 through 100. The default value is 5.

---

threshold

license-utilization: Specifies the license-utilization percentage threshold for overload situations. If candidates are available, passive calls are disconnected when this threshold is exceeded. *percentage_value* is an integer from 1 through 100. The default value is 80.
max-sessions-per-service-utilization: Specifies a percentage of the maximum sessions per service. If candidates are available, passive calls are disconnected when this threshold is exceeded. *percentage_value* is an integer from 1 through 100. The default value is 80.
tolerance: Specifies the percentage of calls the system disconnects below the values set for the other two thresholds. In either case, a Clear Traps message is sent after the number of calls goes below the corresponding threshold value. *number* is an integer from 1 through 25. The default value is 10.

---

default

When "default" and one of the keywords is added to the command, the policy remains in its current state and the value for the specified keyword is reset to its default value.
When "default" and the command are entered without keywords, the overload-disconnect policy for congestion control is disabled.

---

no congestion-control overload-disconnect

Disables the overload-disconnect policy for congestion control.

Usage

Use this command to set the policy for call disconnects when the chassis experiences call overload.
To verify the congestion-control configuration use **show congestion-control configuration** from the Exec mode.
To set overload-disconnect policies for individual subscribers., see **overload-disconnect** in Subscriber Configuration Mode Commands.

Example

The following command sets an overload-disconnect policy for the chassis in which 5 calls would be disconnected very 5 seconds during an overload situation.

```
congestion-control overload-disconnect interations-per-stage 5
```

Both of the following commands disable the overload-disconnect policy without changing the policy configuration.

```
default congestion-control overload-disconnect
```

or

```
no congestion-control overload-disconnect
```

To instruct the system to stop call disconnects when the number of calls goes down 85% of the total allowed calls for that service, enter both of the following commands to set the max-sessions-per-service-utilization value to 90% and the tolerance value to 5%:

```
congestion-control overload-disconnect threshold max-sessions-per-
service-utilization 90

congestion-control overload-disconnect threshold tolerance 5
```

congestion-control policy

Configures congestion control policies.

Product

All

Privilege

Security Administrator, Administrator

Syntax

congestion-control policy { asngw-service | asnpc-service | cscf-service | fng-service | ggsn-service | ha-service | hnbgw-service | hsgw-service | lma-service | lns-service | mipv6ha-service | pcc-af-service | pcc-policy-service | pcc-quota-service | pdg-service| pdif-service | pdsn-service | pdsnclosedrp-service | pgw-service | phsgw-service | phspc-service | sgsn-service | sgw-service } action { drop | none | redirect | reject }

congestion-control policy mme-service action { drop | none | reject | report-overload { permit-emergency-sessions | reject-new-sessions | reject-non-emergency-sessions } enodeb-percentage *percentage* **}**

default congestion-control policy { asngw-service | asnpc-service | cscf-service | fng-service | ggsn-service | ha-service | hnbgw-service | hsgw-service | lma-service | lns-service | mipv6ha-service | mme-service | pcc-af-service | pcc-policy-service | pcc-quota-service | pdg-service | pdif-service | pdsn-service | pdsnclosedrp-service | pgw-service | phsgw-service | phspc-service | sgsn-service | sgw-service }

default congestion-control policy *service*

Sets the congestion policy action for the selected service to its default value.

asngw-service

Sets the congestion policy action for the ASN-GW service.

asnpc-service

Sets the congestion policy action for the ASN PC-LR service.

cscf-service

Sets the congestion policy action for the CSCF service.

fng-service

Sets the congestion policy action for the FNG service.

ggsn-service

Sets the congestion policy action for the GGSN service.

ha-service

Sets the congestion policy action for the HA service.

hnbgw-service

Sets the congestion policy action for the HNB-GW service.
Supported policy actions are:

- **drop**: Specifies that the system is to drop incoming packets containing new session requests.
- **none**: Specifies that the system is take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

lma-service

Sets the congestion control policy action for the LMA service

lns-service

Sets the congestion policy action for the LNS service.

mipv6ha-service

Sets the congestion policy action for the MIPv6-HA service.

mme-service

Sets the congestion control policy for action to take when subscriber sessions exceeds the defined threshold limit.
For MME type of session/calls **redirect** action is not supported.

pcc-af-service

Sets the congestion policy action for the PCC Application Function (AF) service.
Supported policy actions are:

- **drop**: Specifies that the system is to drop incoming packets containing new session requests.
- **none**: Specifies that the system is take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

pcc-policy-service

Sets the congestion policy action for the PCC Policy service.
Supported policy actions are:

- **drop**: Specifies that the system is to drop incoming packets containing new session requests.
- **none**: Specifies that the system is take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

pdg-service

Sets the congestion policy action for the PDG service.

pdif-service

Sets the congestion policy action for the PDIF service.

pdsn-service

Sets the congestion policy action for the PDSN service.

sgsn-service

Sets the congestion policy action for the SGSN service.

action { drop | none | redirect | reject }

Defines what policy action is taken:

- **drop**: Specifies that the system is to drop incoming packets containing new session requests. (PDSN, GGSN, ASN GW, LMA, MME, and ASN PC and HA only)
- **none**: Specifies that the system is take no action. This is the default for PDIF-service.
- **redirect**: Specifies that the system is to redirect new session requests to an alternate device. (PDSN and HA only)

  Important: If this option is used, the IP address of the alternate device must be configured using the **policy overload redirect** command that is part of the service configuration. Note that this option can not be used in conjunction with GGSN and MME services.

- **reject**: Specifies that the system processes new session request messages and responds with a reject message. (For PDSN and HA, the reply code is 130, "insufficient resources". For the GGSN, the reply code is 199, "no resources available".)

report-overload { permit-emergency-sessions | reject-new-sessions | reject-non-emergency-sessions } enodeb-percentage *percentage*

Important: This set of keywords is supported only by the MME.

Enables the MME to report overload conditions to eNodeBs and take additional action to alleviate congestion situations.

permit-emergency-sessions: Specifies that only emergency sessions are allowed to access the MME during the overload period.

reject-new-sessions: Specifies that all new sessions destined for the MME will be rejected during the overload period.

reject-non-emergency-sessions: Specifies that all non-emergency sessions will be rejected during the overload period.

enodeb-percentage *percentage*: Configures the percentage of known eNodeBs that will receive the overload report. *percentage* must be an integer from 1 to 100.

Usage

Congestion policies can be configured for each service. When congestion control functionality is enabled, these policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

Example

The following command configures a congestion control policy of reject for PDSN services:

```
congestion-control policy pdsn-service action reject
```

The following command configures a congestion control policy of reject for MME services:

```
congestion-control policy mme-service action reject
```

congestion-control threshold

Configures the congestion control threshold values that are to be monitored.

Product

All

Privilege

Security Administrator, Administrator

Syntax

congestion-control threshold { license-utilization *percent* **| max-sessions-per-service-utilization** *percent* **| message-queue-utilization** *percent* **| message-queue-wait-time** *time* **| port-rx-utilization** *percent* **| port-specific {** *slot/port* **| all } [tx-utilization** *percent* **] [rx-utilization** *percent* **] | port-tx-utilization** *percent* **| service-control-cpu-utilization** *percent* **| system-cpu-utilization** *percent* **| system-memory-utilization** *percent* **| tolerance** *percent* **}**

default congestion-control threshold { license-utilization | max-sessions-per-service-utilization | message-queue-utilization | message-queue-wait-time | port-rx-utilization | port-specific | tx-utilization | rx-utilization | port-tx-utilization | service-control-cpu-utilization | system-cpu-utilization | system-memory-utilization | tolerance }

no congestion-control threshold port-specific { *slot/port* **| all }**

no congestion-control threshold port-specific { *slot/port* **| all } [rx-utilization** *percent* **] [tx-utilization** *percent* **]**

no congestion-control threshold { message-queue-utilization | message-queue-wait-time | port-rx-utilization *percent* **| port-tx-utilization percent | service-control-cpu-utilization | system-cpu-utilization | system-memory-utilization }**

---

default congestion-control threshold *keyword*

Sets the threshold keyword to its default value.

---

no congestion-control threshold port-specific { *slot/port* **| all }**

This command disables port specific threshold monitoring on the specified port or on all ports.
slot/port: Specifies the port for which port specific threshold monitoring is being configured. The slot and port must refer to an installed card and port.
all: Set port specific threshold monitoring for all ports on all cards.

---

license-utilization *percent*

Default: 100
The percent utilization of licensed session capacity as measured in 10 second intervals.
percent can be configured to any integer value from 0 to 100.

---

max-sessions-per-service-utilization *percent*

Default: 80

The percent utilization of the maximum sessions allowed per service as measured in real-time. This threshold is based on the maximum number of sessions or PDP contexts configured for the a particular service. (Refer to the **bind** command for the PDSN, GGSN, SGSN, or HA services.)
percent can be an integer from 0 through 100.

message-queue-utilization *percent*

Default: 80
The percent utilization of the Demux Manager software task's message queue as measured in 10 second intervals. The queue is capable of storing a maximum of 10000 messages.
percent can be an integer from 0 through 100.

message-queue-wait-time *time*

Default: 5
The maximum time (in seconds) messages can be held in queue as measured by packet time stamps.
time is measured in seconds and can be an integer from 1 through 30.

Important: In the event that this threshold is crossed, an SNMP trap is not triggered. The service congestion policy invocation resulting from the crossing of this threshold is enforced only for the packet that triggered the action.

[no] port-rx-utilization *percent*

Default: 80
The average percent utilization of port resources for all ports by received data as measured in 5 minute intervals.
percent can be an integer from 0 through 100.

[no] port-specific { *slot/port* **| all } [rx-utilization** *percent* **] [tx-utilization** *percent***]**

Default: Disabled
Sets port-specific thresholds. If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is applied system-wide.
slot/port: Specifies the port for which port-specific threshold monitoring is being configured. The slot and port must refer to an installed card and port.
all: Set port specific threshold monitoring for all ports on all cards.
rx-utilization *percent*: Default 80%. The average percent utilization of port resources for the specified port by received data as measured in 5 minute intervals. *percent* must an integer from 0 through 100.
tx-utilization *percent*: Default 80%. The average percent utilization of port resources for the specified port by transmitted data as measured in 5-minute intervals. *percent* must be an integer from 0 through 100.

[no] port-tx-utilization *percent*

Default: 80
The average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.
percent can be an integer from 0 through 100.

service-control-cpu-utilization *percent*

Default: 80
The average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

percent can be an integer from 0 through 100.

system-cpu-utilization *percent*

Default: 80
The average percent utilization for all PSC/PSC2 CPUs available to the system as measured in 10-second intervals.
percent can be an integer from 0 through 100.
This threshold setting can be disabled with **no congestion-control threshold system-cpu-utilization** command. In case later you want to enable the same threshold setting **congestion-control threshold system-cpu-utilization** command will enable the CPU utilization threshold to preconfigured level.

system-memory-utilization *percent*

Default: 80
The average percent utilization of all CPU memory available to the system as measured in 10-second intervals.
percent can be an integer from 0 through 100.

tolerance *percent*

Default: 10
The percentage under a configured threshold that dictates the point at which the condition is cleared.
percent can be an integer from 0 through 100.

Usage

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). These thresholds function in a similar fashion to the operation thresholds that can be configured for the system (as described in later in this chapter). The primary difference is that when these thresholds are reached, not only is an SNMP trap generated (starCongestion), but a service congestion policy is invoked as well.
The tolerance parameter establishes the threshold at which the condition is cleared. An SNMP trap (starCongestionClear) is generated for the clear condition, as well.

Example

The following command configures a system CPU utilization threshold of 75%.

```
congestion-control threshold system-cpu-utilization 75
```

This setting will remain in configuration unless you specify another threshold value in place of 75. This threshold setting can be disabled with **no congestion-control threshold system-cpu-utilization** command but cannot be removed from configuration. Later if you want to enable the previously configured threshold value of *75* percent, you only need to enter the **congestion-control threshold system-cpu-utilization** command without specifying any threshold value. It will enable the CPU utilization threshold to preconfigured level of *75* percent.
For example, **no congestion-control threshold system-cpu-utilization** disables the configured threshold setting and **congestion-control threshold system-cpu-utilization** again enables the threshold setting of 75%.
The following command configures a threshold tolerance of 5%:

```
congestion-control threshold tolerance 5
```

In the above examples, the starCongestion trap gets triggered if the system CPU utilization goes above 75% and the starCongestionClear trap gets triggered if it reaches or goes below 70%.

content-filtering category database directory

This command configures the base directory to be used for storing all content-rating databases that are required for Category-based Content Filtering application.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

content-filtering category database directory path *directory_path*

default content-filtering category database directory path

default

Specifies the default base directory and directory path for Category-based Content Filtering application.

directory_path

Default: /pcmcia1/cf
Specifies the base directory and its path to store all of the full or incremental content rating databases for the Category-based Content Filtering application.
directory_path must be an alphanumeric string of 1 through 255 characters.

Usage

Use this command to specify the directory and its path to download all full or incremental category-rating databases to be used for the Category-based Content Filtering application.
Merging of incremental database can be done as part of the database upgrade process preformed with **upgrade content-filtering category database** command in the Executive Mode.

Example

The following command configures the */flash/cf_temp/DB* as the base directory to download all full and incremental content-rating databases for content filtering application.

```
content-filtering category database directory path /flash/cf_temp/DB
```

content-filtering category database max-versions

This command configures the number of full content-rating databases to maintain/archive in the base directory for category-based content filtering application.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

content-filtering category database max-versions *num_archive*

default content-filtering category database max-versions

default

Sets the default number of full databases for specified directory path/location.

num_archive

Default: 2
Specifies the maximum number of database to be archived or maintained in the specific location.
num_archive must be an integer from 1 through 3.

Usage

Use this command to set the number of full content-rating database to be maintained in the specified directory path with the base file name specified using the **content-filtering database override file** command. The specified directory path is the location specified using the **content-filtering category database directory path** command.

Example

The following command configures the system to maintain *3* full content-rating databases for category-based content filtering application.

```
content-filtering category database max-versions 3
```

content-filtering category database override

This command specifies the name of a file to be used by the category-rating database load process for category-based content filtering application.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

content-filtering category database override file *file_name.extension*

default content-filtering category database override file

default

Sets the default content rating database file name; for example, optcmd.bin.

file *file_name.extension*

Specifies the header of the file in the database directory path location to determine the newest full database. *file_name* must be an alphanumeric string of up to 10 characters with an extension of 3 characters after a period (.) as *extension*.

Usage

Use this command to configure the category-rating database file name to determine the newest version of full database. A process called "**LOAD_DATABASE**" invokes during the system startup or the database upgrade process by **upgrade content-filtering category database** command in Executive Mode. This process examines the header of each of the files in the database folder specified by **content-filtering category directory path** command in this mode.
Note that by default system examines the header of those files only which begins with the string "OPTCMDB" and having extension ".bin".

Example

The following command configures the system to examine the header of files that begins with *CF_sta.DB* only for content filtering application.

```
content-filtering category database override file CF_sta.DB
```

context

Enters the Context Configuration mode or is used to add or remove a specified context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

context *name* **[-noconfirm]**

no context *name*

no

Removes the specified context from the configuration.

name

Specifies the name of a context to enter, add, or remove. When creating a new context, the context name must be unique.

Important: When creating a new context, the *context name* specified must not conflict with the name of any existing context or domain names.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Configure contexts or remove obsolete contexts.

Important: A maximum of 64 contexts may be created.

Example

context *sampleContext*

no context *sampleContext*

crash enable

Enables or disables the copying of crash data to a specified location.

Product

All

Privilege

Security Administrator, Administrator

Syntax

crash enable [encrypted] url *crash_url* **[filename-pattern** *pattern* **] [restrict** *mbyte* **]**

no crash enable

no

Removes the specified context from the configuration.

Important: System crash information is generated and stored in the crash list even when the **no** keyword is specified. The information maintained in the crash lists is minimal crash information when the **no** keyword has been specified.

encrypted

Indicates that the URL encrypted for security reasons.

filename-pattern *pattern*

The **filename-pattern** is a an alphanumeric string containing any or all of the following variables:

- *%hostname%* - The system hostname.
- *%ip%* - A SPIO IP address
- *%cpu%* - CPU number
- *%card%* - Card number
- *%time%* - POSIX timestamp in hexadecimal notation
- *%filename%* - Alias for *crash-%card%-%cpu%-%time-core%*
- *%%* - A single *%* sign

If no pattern is specified, the result is the same as the pattern *filename*.
Use '/' characters in the filename pattern part to store crashes in per-system subdirectories.

url *crash_url*

Specifies the location to store crash files. *crash_url* may refer to a local or a remote file. *crash_url* must be entered using the following format:

- **[file:]{/flash|/pcmcia1|/pcmcia2}[/***directory***]/**
- **tftp://{***host***[:***port#***]}[/***directory***]/**
- **[ftp:|sftp:]//[***username***[:***password***]@] {***host***}[:***port#***][/***directory***]/**
- ASR 5000:

- **[file:]{/flash|/pcmcia1|/hd}[/***directory***]/**
- **tftp://{***host***[:***port#***]}[/***directory***]/**
- **[ftp:|sftp:]//[***username***[:***password***]@] {***host***}[:***port#***][/***directory***]/**

Important: Use of the SMC hard drive is not supported in this release.

Important: Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

restrict *mbyte*

Specifies a maximum amount of memory (in megabytes) to use for storing crash files as an integer from 1 through 128. Default: 128
The **restrict** keyword is only applicable to local URLs.

Usage

Enable crashes if there are systems that are not stable and the crash information will be useful for trouble shooting. The remote storage of the crash file reduces the memory utilized on the chassis.

Example

```
crash enable ftp://remoteABC/pub/crash.dmp

crash enable /flash/pub/data/crash.dmp restrict 64

no crash enable
```

cs-network

This command creates/removes an HNB-CS network configuration instance for Femto UMTS access over Iu-CS/Iu-Flex interface between Home NodeB Gateway (HNB-GW) service and CS networks elements; i.e. MSC/VLR. This command also configures an existing HNB-CS network instance and enters the HNB-CS Network Configuration mode on a system.

Product

HNB-GW

Privilege

Administrator

Syntax

cs-network *cs_instance* **[-noconfirm]**

no cs-network *cs_instance*

no

Removes the specified HNB-CS network instance from the system.

Caution: Removing the HNB-CS network instance is a disruptive operation and it will affect all UEs accessing MSC(s) configured in specific CS core network through the HNB-GW service.

Caution: If any HNB-CS Network instance is removed from system all parameters configured in that mode will be deleted and Iu-CS/Iu-Flex interface will be disabled.

cs_instance

Specifies the name of the Circuit Switched Core Networks instance which needs to be associated with the HNB Radio Network PLMN via the HNB RN-PLMN Configuration mode. If *cs_instance* does not refer to an existing HNB-PS network instance, the new HNB-CS network instance is created.
cs_instance must be an alphanumeric string of 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to enter the HNB-CS Network Configuration mode for an existing CS network instance or for a newly defined HNB-CS network instance. This command is also used to remove an existing HNB-CS network instance.
This configuration enables/disables the Iu-CS/Iu-Flex interface on HNB-GW service with CS core network elements; i.e. MSC/VLR.
A maximum of one HNB-CS network instance per HNB-GW service instance which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

Caution: This is a critical configuration. The HNBs cannot access MSC(s) in CS core network without this configuration. Any change to this configuration would lead to disruption in HNB access to CS core network.

Entering this command results in the following prompt:

```
[context_name]hostname(config-cs-network)#
```

The various parameters available for configuration of an HNB-CS network instance are defined in the *HNB-CS Network Configuration Mode Commands* chapter.

Example

The following command enters the existing HNB-CS Network configuration mode (or creates it if it does not already exist) for the instance named *hnb-cs1*:

```
cs-network hnb-cs1
```

The following command will remove HNB-CS network instance *hnb-cs1* from the system without any warning to operator:

```
no cs-network hnb-cs1
```

css acsmgr-selection-attempts

This is a restricted command. In 9.0 and later releases this command is obsolete.

css delivery-sequence

This is a restricted command. In 9.0 and later releases this command is obsolete.

css service

This is a restricted command. In 9.0 and later releases this command is obsolete.

default

Restores the system default values for the specified parameters.

Product

All

Privilege

Security Administrator, Administrator

Syntax

default { autoconfirm | banner [lawful-intercept | motd | pre-login] | boot [delay | interface | nameserver | networkconfig] | card-standby-priority | cli max-sessions | congestion-control | logging { display | filter runtime } | operational-mode | pac-standby-priority | qos npu inter-subscriber traffic { bandwidth | priority [assigned-to dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef }] } | require session recovery | snmp { engine-id | notif-threshold } | system hostname | task { facility sessmgr start | resource cpu-memory-low } | threshold { *value* **} | timestamps | upgrade limit [time] [usage] }**

---

autoconfirm

Restores the autoconfirm behavior to its default of disabled.

---

banner

lawful-intercept - Restores the system default message of the day for SSH CLI sessions.
motd – Restores the system default message of the day banner.
pre-login – Restores the CLI log in banner to the system default.

---

boot [delay | interface | nameserver | networkconfig]

interface | networkconfig - Restores the default boot interface and network configuration options. The keywords **interface** and **networkconfig** are used to restore the default option settings for the interface and network configuration options, respectively.
Defaulting the network configuration boot option removes the network boot option from the boot.sys file. It does not remove the network config options from the configuration file which is managed separately from the boot.sys file.
delay - Removes the boot delay setting (if any). The default for boot delay is “no boot delay”.
nameserver - Removes the nameserver IP address.

---

card-standby-priority

Resets the standby priority of the Packet Services Cards.

---

cli max-sessions

Restores the default value of this command to **no cli max-sessions** which removes the limit on the number of allowed simultaneous CLI sessions on the system.

---

congestion-control

Restores the system’s congestion-control functionality to its default setting of disabled.

logging {display | filter runtime}

display: sets the default level of detail to display for trace log information to the system default.
filter runtime: resets the filtering of logged information to log in real time.

operational-mode

Sets the operational mode of the chassis to the system default.

pac-standby-priority

This parameter has been replaced by the **card-standby-priority** keyword.

qos npu inter-subscriber traffic {bandwidth | priority [assigned-to dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef }] }

Restores the following NPU QoS parameters to their default values:

- **bandwidth**:
- gold: 10%
- silver: 20%
- bronze: 30%
- best-effort: 40%
- **priority**: All DSCP values are mapped to the best-effort priority queue but are not configured.

require session recovery

Resets the session recovery feature to its default setting of disabled.

snmp { engine-id | notif-threshold | system hostname | timestamps }

engine-id: restores the SNMP engine ID to the system default.
notif-threshold: restores the SNMP notification threshold to the system default.

task { facility sessmgr start | resource cpu-memory-low }

facility sessmgr start: Restores the default session manager start policy.
resource cpu-memory-low: Resets the system so that when a CPU runs very low on memory (below 12MB) the most over limit task is killed.

system hostname

Sets the system host name for SNMP use to the system default value.

threshold { *value* }

Restores thresholding values to their default setting. The possible values are:

- **10sec-cpu-utilization**: CPU utilization using a 10 sec average.
- **aaa-acct-archive-size**: AAA accounting archive queue threshold settings
- **aaa-acct-failure**: AAA accounting failure threshold settings
- **aaa-acct-failure-rate**: AAA accounting failure rate threshold settings
- **aaa-auth-failure**: AAA authentication failure threshold settings

- **aaa-auth-failure-rate**: AAA authentication failure rate threshold settings
- **aaa-retry-rate**: AAA retry rate threshold settings
- **aaamgr-request-queue**: AAA manager internal request queue threshold settings
- **call-reject-no-resource**: Calls rejected due to no resources threshold settings
- **call-setup**: Calls setup threshold settings
- **call-setup-failure**: Call setup failure threshold settings
- **contfilt-block**: Content Filtering Blocks threshold settings
- **contfilt-rating**: Content Filtering Ratings threshold settings
- **cpu-available-memory**: CPU available memory threshold settings
- **cpu-load**: PSC/PSC2 CPU load using a 5 minute average measurement
- **cpu-memory-usage**: Percentage of total CPU memory usage
- **cpu-session-throughput**: CPU session throughput threshold settings
- **cpu-utilization**: CPU utilization threshold settings
- **dcca-bad-answers**: Diameter Bad Answers threshold settings
- **dcca-protocol-error**: Diameter Protocol Error threshold settings
- **dcca-rating-failed**: Diameter Rating Failed threshold settings
- **dcca-unknown-rating-group**: Diameter Unknown Rating Group threshold settings
- **diameter**: Diameter threshold settings
- **license**: Session license threshold settings
- **model**: Thresholding model settings
- **monitoring**: Threshold monitoring configuration settings
- **packets-filtered-dropped**: Filtered/dropped packet threshold settings
- **packets-forwarded-to-cpu**: Forwarded packet threshold settings
- **pdif-current-sessions**: Threshold monitoring for all current PDIF sessions.
- **pdif-current-active-sessions**: Threshold monitoring for only the currently-active PDIF sessions.
- **per-service-ggsn-sessions**: The number of GGSN sessions per GGSN service
- **per-service-gprs-sessions**: The number of GPRS sessions per GPRS service
- **per-service-gprs-pdp-sessions**: The number of PDP contexts per GPRS service
- **per-service-ha-sessions**: The number of HA sessions per HA service
- **per-service-lns-sessions**: The number of LNS sessions per LNS service
- **per-service-pdsn-sessions**: The number of PDSN sessions per PDSN service
- **per-service-sgsn-sessions**: The number of SGSN sessions per SGSN service
- **per-service-sgsn-pdp-sessions**: The number of PDP contexts per SGSN service
- **poll**: Threshold polling interval configuration settings
- **total**: Total subscriber threshold settings
- **total-ggsn-sessions**: Total GGSN sessions for all GGSN services in the system

- **total-gprs-sessions**: Total GPRS sessions per for all GPRS services in the system
- **total-gprs-pdp-sessions**: Total PDP contexts for all GPRS services in the system
- **total-ha-sessions**: Total HA sessions for all HA services in the system
- **total-lns-sessions**: Total LNS sessions for all LNS services in the system
- **total-pdsn-sessions**: Total PDSN sessions for all PDSN services in the system
- **total-sgsn-sessions**: Total SGSN sessions per for all SGSN services in the system
- **total-sgsn-pdp-sessions**: Total PDP contexts for all SGSN services in the system

timestamps

Resets the inclusion of timestamps in command.

upgrade limit [time] [usage]

Sets upgrade limit values to the defaults. If the optional keywords are not specified all values are reset to their defaults.
time: Resets the maximum time a session may exist during a software upgrade to the default of 120.
usage: Resets the minimum number of sessions before closing the sessions during a software upgrade to the system default of 100.

Usage

Restore system defaults to aid in trouble shooting or just prior to modifying additional configuration options.

Example

```
default banner motd

default boot

default logging display

default system hostname

default upgrade limit time
```

diameter-proxy ram-disk

This command configures the amount of extra RAM disk space in MB to be allocated to Diamproxy task when local storage (hard disk) is enabled.

Product

SGW, PGW, HSGW

Privilege

Security Administrator, Administrator

Syntax

diameter-proxy ram-disk mb *space_mb*

default diameter-proxy ram-disk mb

default

Configures the default setting.
Default: 32 MB

mb space_mb

Specifies the storage space in MB.
space_mb must be an integer from 10 through 256.

Usage

Specifies the additional storage space to be allocated to Diamproxy for file write, in MB. The specified memory in MB is added to the existing memory allocated to Diamproxy only if HDD storage is enabled. By default, 32 MB is additionally allocated.

Example

The following command specifies that *100* MB of additional storage space be allocated to the Diamproxy task:

```
diameter-proxy ram-disk mb 100
```

ecmp-lag hash

This command provides the configuration to select source Boxer Internal Address (SBIA) as the input to the hashing function for ECMP-LAG distribution.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

```
[no] ecmp-lag hash use-sbia-only
```

no

Disables the hashing function selection and sets the system to use IP Source Address, IP Destination Address, IP Protocol and Source BIA as inputs to the hashing algorithm for ECMP-LAG distribution.

Usage

Use this command to allow the operator to change the way hashing works in deciding which link to use for ECMP and Link Aggregation. In the default hashing algorithm the IP Source Address, IP Destination Address, IP Protocol and Source BIA are used in the hashing function. When “use-sbia-only” option is selected, only the Source BIA is used in the hashing function.

Caution: When using ECMP-LAG on a HNB-GW, this configuration is **mandatory** for standalone HNB-GW deployment and highly recommended in other deployment scenarios where HNB-GW is used in combination with other services.

Example

The following command enables the SBIA as input to hash function for ECMP-LAG on the HNB-GW:

```
ecmp-lag hash use-sbia-only
```

The following commands sets the hashing function to use standard inputs for ECMP-LAG on HNB-GW:

```
no ecmp-lag hash use-sbia-only
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

enforce imsi-min equivalence

Enables the PDSN/HA to treat IMSI and MIN as the same for identifying the PDSN/HA session.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

```
enforce imsi-min equivalence

[ no | default ] enforce imsi-min equivalence
```

`[ no | default ]`

Disables the PDSN/HA from treating IMSI and MIN as the same for identifying the PDSN/HA session.
Default: Disabled.

Usage

Generally on an HA, the IMSI and MIN are treated as different and hence the RRQs with 1x and DO PDSNs are processed as different sessions. You can use this feature to treat the IMSI and MIN with the matching lower 10-digit as the same for identifying a session. The 10-digit MIN and the 15-digit IMSI are treated as equivalent for the purpose of matching sessions if the lower 10 digits are the same. Any handoff from 1x to DO or vice-versa is treated as the same session if the NAI and HoA also match. If the NAI and/or HoA do not match, then the duplicate IMSI session detect and terminate feature is applicable.
Generally on a PDSN, the IMSI and MIN are treated as different and hence RP messages from 1x and DO PDSNs are processed as different sessions. You can use this feature to treat the IMSI and MIN with the matching lower 10-digit as the same for identifying a session. The 10-digit MIN and the 15-digit IMSI are treated as equivalent for the purpose of matching PDSN sessions if the lower 10 digits are the same. Any handoff from 1x to DO or vice-versa is treated as the same session.

Example

To monitor or clear subscriber session information filtered by on IMSI/MIN refer to the **`show subscribers msid`** command.

Important: This command must be executed at startup only and will not take effect when reconfigured without rebooting.

Example

The following command enables the treatment of the IMSI and MIN as the same for identifying the session:

```
enforce imsi-min equivalence
```

Either of the following commands disables the treatment of the IMSI and MIN as the same for identifying sessions:

```
no enforce imsi-min equivalence

default enforce imsi-min equivalence
```

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

fa-spi-list

Replaces a duplicate Foreign Agent- Security Parameter Index (FA-SPI) remote address list applied to multiple FA services with a list name.

Product

All

Privilege

Security Administrator, Administrator

Syntax

fa-spi-list *fa_spi_list*

fa_spi_list

Remote address list name expressed as an alphanumeric string of 1 through 64 characters.

Usage

Use this command to Replace duplicate FA-SPI remote address list applied to multiple FA or HA services with a list name.

Example

The following command configures the list FA SPI list to *fa-list2*:

```
fa-spi-list fa-list2
```

global-title-translation address-map

Creates an instance of a Global Title Translation (GTT) address-map, a database, for global titles (ISDN-type address) used for SCCP routing. Upon creating the instance, the system enters global title translation address-map configuration mode. For the commands to configure the database, go to the *Global Title Translation Address-Map Configuration Mode Commands* chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

global-title-translation address-map instance *instance*

no global-title-translation address-map instance *instance*

no

Removes the specified GTT address-map database from the SCCP portion of the configuration.

instance

This value uniquely identifies a specific instance of a GTT address-map.
instance must be an integer from 1 through 4096.

Usage

Create a GTT address-map with a unique identifier and enter the GTT address-map configuration mode.

Example

```
global-title-translation address-map instance 324
```

global-title-translation association

Creates an instance of a Global Title Translation (GTT) association which defines the rules for handling global title translation. Upon creating the instance, the system enters global title translation association configuration mode. For the commands to configure the rules, go to the *Global Title Translation Association Configuration Mode Commands* chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

global-title-translation association instance *instance*

no global-title-translation association instance *instance*

no

Removes the specified instance of a GTT association from the SCCP portion of the configuration.

instance

This value uniquely identifies a specific instance of a GTT association.
instance must be an integer from 1 through 16.

Usage

Create a GTT association with a unique identifier and enter the GTT association configuration mode.

Example

```
global-title-translation association instance 2
```

gtpp compression-process

This command configures the maximum number of child compression processes that AAA proxy can have. This command is only applicable to the ASR 5000 platform.

Product

GGSN, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp compression-process *max_number*

default gtpp compression-process

default

Restores the system to the default settings for the number of child compression processes allowed.

max_number

Specifies the maximum number of child processes. The default is 1
max_number: must be an integer from 1 through 4.

Usage

This command configures the maximum number of child compression processes that AAA proxy can have only if hard disk storage is enabled.

Example

```
gtpp compression-process 3
```

gtpp ram-disk-limit

This command configures additional storage space to be allocated for writing files. This command is only applicable to the ASR 5000 platform.

Product

GGSN, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp ram-disk-limit mb *mega_bytes*

default gtpp ram-disk-limit

default

Restores the system to the default settings of 32 MB of storage.

mb *mega_bytes*

Specifies the number of megabytes of storage allocated for files.
mega_bytes: must be an integer from 10 through 256. The default is 32 MB.

Usage

The memory specified with this command would be added to the existing memory allocated to the AAA proxy only if hard disk storage is enabled.

Example

```
gtpp ram-disk-limit mb 256
```

gtpp single-source

Configures the system to reserve a CPU for performing a proxy function for accounting.

Product

GGSN, SGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
gtpp single-source [ centralized-lrsn-creation | private-extensions ]

no gtpp single-source
```

centralized-lrsn-creation

Defines Log Record Sequence Number (LRSN) generation at proxy. The AAA proxy will generate the LRSN for all CDR types generated by either the GGSN or the SGSN.
Default: disabled

private-extensions

This optional keyword enables the proprietary use of customer-specific GTPP extensions.
If **private-extensions** is not configured, all customer specific private extensions related to GTPP message transfer with CGF and recovery through GSS are disabled.

Important: In order for the customer-specific extensions to work properly, the **gtpp max-pdu-size** command in the Context Configuration Mode should be set to 65400 and the **gtpp server** command's **max** value should be set to "1".

no

Disables GTPP single-sourcing. This is the default setting.

Caution: Entering this command while PDP contexts are in process could cause the loss of pending CDRs. The configuration must be saved and the chassis reloaded for this option to take effect.

Usage

When GTPP single-sourcing is enabled, the system's AAA proxy function generates requests to the accounting server using a single UDP source port number, instead of having each AAA Manager generate independent requests with unique UDP source port numbers. This is accomplished by the AAA Managers forwarding their GTPP PDUs to the AAA Proxy function that runs on a reserved packet processing card CPU. Since a packet processing card CPU is being reserved, fewer Session Managers and AAA Managers will be started on that card.

Caution: This command must be entered prior to the configuration of other services. Specifying it later may return an error due to a lack of CPU availability.

Example

The following command enables GTPP single-sourcing with the use of private GTPP extensions:

```
gtpp single-source private-extensions
```

The following command disables GTPP single-sourcing:

```
no gtpp single-source
```

ha-spi-list

Replaces a duplicate Home Agent-Security Parameters Index (HA-SPI) remote address list applied to multiple HA services with a list name.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ha-spi-list *ha_spi_list*

ha_spi_list

Remote address list name expressed as an alphanumeric string of 1 through 64 characters.

Usage

Use this command to Replace duplicate HA-SPI remote address list applied to multiple HA services with a list name.

Example

The following command configures the list HA SPI list to *ha-list2*:

```
ha-spi-list ha-list2
```

hd raid

Provides access to a local RAID hard drive configuration mode in order to manage parameters supporting local storage of records.

Product

All

Privilege

Security Administrator, Administrator

Syntax

hd raid

raid

Provides access to the HD RAID configuration mode in order to manage the RAID on the ASR 5000 SMC hard drive.

Usage

Enters the HD RAID configuration mode.
Entering this command results in the following prompt:

```
[context_name]hostname(config-hd-raid)#
```

HD RAID Configuration Mode commands are defined in the HD RAID Configuration Mode Commands chapter.

Example

The following command opens the hd-raid mode:

```
hd raid
```

hd storage-policy

Provides access to the local hard drive configuration mode in order to manage parameters supporting local storage of records.

Product

GGSN, SGSN, HSGW, P-GW, S-GW

Privilege

Administrator

Syntax

[no] hd storage-policy *name*

no

Removes a configured HD storage policy from the system.

storage-policy *name*

Specifies a name for an HD storage policy and then enters the HD Storage Policy Configuration Mode. *name* must be an alphanumeric string of 1 through 63 characters.

Usage

Creates a new policy or specifies an existing policy and enters the HD Storage Policy Configuration Mode. Entering this command results in the following prompt:
[*context_name*]*hostname*(config-hd-storage-policy)#
HD Storage Policy Configuration Mode commands are defined in the HD Storage Policy Configuration Mode Commands chapter.

Example

The following command creates an HD storage policy named *policy3* and enters the HD Storage Policy Configuration Mode:

```
hd storage-policy policy3
```

high-availability

Configures the speed for detection of packet processing card task failures.

Product

PDSN, GGSN, ASN GW

Privilege

Security Administrator, Administrator

Syntax

```
high-availability fault-detection speed { aggressive | normal }

default high-availability fault-detection speed
```

{ aggressive | normal }

Default: **normal**

- **aggressive**: Initiates packet processing card failover without performing additional checks.
- **normal**: Initiates packet processing card failover after additional checks are performed.

Usage

Use this command to increase the fault detection speed for faster switchovers after a packet processing card task failure.

Setting fault detection speed to aggressive will trigger packet processing card failover as soon as possible if a potential failure is detected. Aggressive mode will reduce the duration of subscriber outages caused by a failed packet processing card if session recovery is enabled.

Aggressive mode also bypasses most information gathering steps and logs that can be used to determine the root cause of the failure.

In normal mode, additional checks are performed before triggering a packet processing card failover to ensure that the card has actually failed. In aggressive mode these checks are bypassed so that session recovery can start as soon as possible. These additional checks reduce the likelihood of a false positive failure.

Example

The following command sets the fault detection speed for packet processing card tasks to **aggressive**:

```
high-availability fault-detection speed aggressive
```

hybrid-mode

Enables an ASR 5000 chassis to run a mix of Packet Services Cards (PSCs) and PSC Type A (PSCAs). When enabled, PSCAs will boot and be compatible with the PSCs as long as encryption services are disabled. The default is to run the chassis in non-hybrid mode; PSCAs will not boot when inserted in the chassis.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] hybrid-mode [force]
```

no

Returns the chassis to non-hybrid mode. PSCAs will not boot.

force

Always updates the configuration, even if the encryption services could not be disabled. However, the PSC and PSCA cards will continue to be incompatible until encryption services are manually disabled.

Usage

To allow a chassis to run in PSC/PSCA hybrid-mode with encryption services disabled you must configure **hybrid-mode force** once.
To go from hybrid mode to non-hybrid mode, you must enter the **no hybrid-mode force** command. Non-hybrid chassis mode allows encryption services to be started through the appropriate CLI commands. However, all PSCAs in the chassis will be disabled.
For additional information, see the *ASR 5000 Installation Guide*.

Example

The following command enables the chassis to run a mix of PSCs and PSCAs without encryption services:

```
hydrid-mode force
```

imei-profile

Creates an instance of an International Mobile Equipment Identity (IMEI) profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] imei-profile *imei_profile_name*

no

Deletes the IMEI profile instance from the configuration.

imei_profile_name

Specifies the name of the IMEI profile as an alphanumeric string of 1 through 64 characters.

Usage

Use this command to create an instance of an IMEI profile and to enter the IMEI Profile Configuration mode. An IMEI profile is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy. See the *IMEI Profile Configuration Mode Commands* chapter for information regarding the definition of the rules contained within the profile and the use of the profile.

Important: An IMEI profile is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what IMEI profiles have already been created, return to the Exec mode and enter the **show imei-profile all** command.

Example

The following command creates a configuration instance of an IMEI profile:

```
imei-profile imeiprof1
```

license

Configures the session license key.

Product

All

Privilege

Security Administrator, Administrator

Syntax

license key *key_value* **[-force] session-limit**

no license key *key_value* **[-force] session-limit**

no

Removes the license key(s) installed.

key *key_value*

Installs the license key specified by *key_value*. *key_value* is provided by Cisco operations staff.

session-limit

Use this keyword to suppress fail-over calls from being rejected if the licensed threshold is crossed.

Important: This is a customer-specific command that is available for HA, PDSN, EHA, and PDIF. Please contact your local Cisco sales representative for more information.

-force

Sets the license key even if resources are not available. The system supports the dynamic resizing of demultiplexor software tasks based on the licensed session capacity and feature type. When installing a license, the system automatically attempts to resize currently functioning tasks. Warning messages are displayed if there is an issue. Though its use is not recommended, the **-force** keyword can be used to suppress these warning messages.

Caution: Use of this option is not recommended.

Usage

Install or update system session keys when necessary due to expiration and/or capacity needs.

Example

license key *sampleKeyValue*

no license key

line

Enters the terminal display line configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
line
```

Usage

Change the terminal display configuration based upon the users own terminal characteristics.

link-aggregation

Configures the Link Aggregation system priority. This parameter is usually changed to match the feature requirements of the remote switch.

Product

WiMAX, PDSN, HA, FA, GGSN, SGSN

Privilege

Security Administrator, Administrator

Syntax

link-aggregation { system-mac [MAC | auto] | system-priority *priority* **} [-noconfirm]**

{ default | no } link-aggregation { system-mac | system-priority } [-noconfirm]

default

Resets the configuration to the default.

link-aggregation system-mac { MAC | auto } *priority*

Sets the system MAC address used along with the system priority to form the system ID.
MAC is a manually entered MAC address (six groups of two hexadecimal digits separated by hyphens).
Auto is the default and is the LAG master port's MAC address.

link-aggregation system-priority *priority*

This command sets the system priority used by LACP to form the system ID.
priority is a hexadecimal value from 0x0000 through 0xFFFF.
Default system priority value is 0x8000 (32768).

-noconfirm

Instructs the system to execute the command without additional prompting for command confirmation.

Usage

The system MAC address (6 bytes) and system priority (2 bytes) combine to form the system ID. A system consists of a packet processing card and its associated QGLC(s) or XGLCs. The highest system ID priority (the lowest number) handles dynamic changes.
For additional usage and configuration information for the link aggregation feature, go to Configuring Link Aggregation in the *System Administration Guide*.

Important: Not supported on all platforms

Example

The following command configures the link aggregation system-priority to 10640 (*0x2990*):

```
link-aggregation system-priority 0x2990
```

local-policy-service

This command enables creating, configuring, or deleting a local QoS policy.

Product

P-GW

Privilege

Security Administrator, Administrator

Syntax

local-policy-service *name* **[-noconfirm]**

no local-policy-service *name*

name

Specifies name of the local QoS policy service as an alphanumeric string of 1 through 63 characters.

Important: The *name* must be unique across all contexts.

If the named local QoS policy service does not exist, it is created, and the CLI mode changes to the Local Policy Service Configuration Mode wherein the local QoS policy service can be configured.
If the named local QoS policy service already exists, the CLI mode changes to the Local Policy Service Configuration Mode for that local QoS policy service.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

no

Deletes the specified local QoS policy service from the system.

Usage

Use this command to specify a local QoS policy service name to allow configuration of a local QoS policy service.

Important: This feature is license dependent. Please contact your local sales representative for more information.

A local QoS policy service can be used to control different aspects of a session, such as QoS, data usage, subscription profiles, or server usage, by means of locally defined policies.
Local QoS policies are triggered when certain events occur and the associated conditions are satisfied. For example, when a new call is initiated, the QoS to be applied for the call could be decided based on the IMSI, MSISDN, and APN.

Important: A maximum of 16 local QoS policy services are supported.

Entering this command results in the following prompt:

```
[context_name]hostname(config-local-policy-service)#
```

Local Policy Service Configuration Mode commands are defined in the *Local Policy Service Configuration Mode Commands* chapter.

Example

The following command creates a local QoS policy service named *lctest* and enters the Local Policy Service Configuration Mode:

```
local-policy-service lctest
```

local-user allow-aaa-authentication

Enables or disables the use of administrative accounts other than local-user administrative accounts.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] local-user allow-aaa-authentication
```

no

Disables administrative user accounts other than local-user accounts.

default

Returns this parameter to its default setting of enabled.

Usage

Local-user administrative accounts are separate from other administrative user accounts configured at the context level (Security Administrator, Administrator, Operator, and Inspector).
Context-level administrative users rely on the system's AAA subsystems for validating user names and passwords during login. This is true for both administrative user accounts configured locally through a configuration file or on an external RADIUS server.
Since the T1.276-2003 password security mechanisms are supported only for local-user administrative accounts and not for the AAA-based administrative accounts, this command provides a mechanism for disabling AAA-based administrative accounts.
By default, AAA-based administrative accounts are allowed.

Example

The following command forces the system to authenticate local-user accounts based only on the information in the security account file on its CompactFlash:

```
no local-user allow-aaa-authentication
```

local-user lockout-time

Configures the lockout period for local-user administrative accounts.

Product

All

Privilege

Security Administrator, Administrator

Syntax

local-user lockout-time *time*

default local-user lockout-time

default

Restores the parameter to its default setting.

time

Default: 60
Specifies the amount of time (in minutes) that must elapse before a previously locked-out local-user account can attempt to login again. *time* is an integer from 1 through 10080.

Usage

Local-user administrative accounts can become locked for reasons such as exceeding the configured maximum number of login failures.
Once an account is locked, this parameter specifies the lockout duration. Once the amount of time configured by this parameter has elapsed, the local-user can once again attempt to login.

Example

The following command configures a lockout time of *120* minutes (2 hours):

```
local-user lockout-time 120
```

local-user max-failed-logins

Configures the maximum number of failed login attempts a local-user can have before their account is locked out.

Product

All

Privilege

Security Administrator, Administrator

Syntax

local-user max-failed-logins *number*

[default | no] local-user max-failed-logins

no

Disables this functionality.

default

Restores this parameter to its default setting.

number

Default: 5
Specifies the maximum number of times a local-user could experience a login failure before their account is locked out. *number* is an integer from 2 through 100.

Usage

This command configures the maximum number of failed login attempts a local-user can have before their account is locked out. For example if, this parameter is configured to "3" then after the third failed login attempt, the account would be locked.

Important: Local-user accounts can be configured to either enforce or reject a lockout due to the maximum number of failed login being reached. Refer to the **local-user username** command for more information.

Refer to the **local-user lockout-time** command for more information.

Example

The following command configures a maximum of three login attempts:

```
local-user max-failed-logins 3
```

local-user password

Configures local-user administrative account password properties.

Product

All

Privilege

Security Administrator, Administrator

Syntax

local-user password { [complexity { ansi-t1.276-2003 | none }] [history length *number* **[duration** *days* **]] [max-age** *days* **] [min-change-char** *number* **] [min-change-interval** *days* **] [min-length** *number* **] }**

no local-user password { [history] [max-age] [min-change-interval] }

default local-user password { [complexity] [history] [max-age] [min-change-char] [min-change-interval] [min-length] }

no

Disables the specified parameter.

default

Restores the specified parameter to its default setting.

[complexity { ansi-t1.276-2003 | none }]

Default: ansi-t1.276-2003
Specifies the password strength as one of the following:

- **ansi-t1.276-2003:** If this option is selected, the following rules are enforced:
- Passwords may not contain the username or the reverse of the username
- Passwords may contain no more than three of the same characters used consecutively
- Passwords must contain at least three of the following:
  - uppercase alpha character
  - lowercase alpha character
  - numeric character
  - special character
- **none:** No additional password checks are performed.

[history length *number* **[duration** *days* **]]**

Default: length is 5
Specifies the number of previous password entries kept in the history list maintained by the system. A password cannot be reused if it is one of the entries kept in the history list unless the time it was last used was more than the number of days specified by the **duration** keyword.
If the duration keyword is not used, the only check performed by the system is that it is not in the history list.

number is the number of entries for each account stored in the history list entered as an integer from 1 through 100. *days* is the number of days during which a password can not be reused entered an integer from 1 through 365.

[max-age *days* **]**

Default: 90
Specifies the maximum age for a password. Users logging in with a password older than the specified limit are locked out. Once the lockout period expires, at their next login attempt, they are prompted to change their password before accessing the CLI.

Important: Local-user accounts can be configured to either enforce or reject a lockout due to a password's maximum age being reached. Refer to the **local-user username** command for more information.

days is the number of days that passwords remain valid entered as an integer from 1 through 365.

[min-change-char *number* **]**

Default: 2
Specifies the minimum number of characters that must be changed (in comparison to the current password) when a user changes their password.

Important: Changes in password length are counted as "character" changes. For example: changing a password from "password" to "passwo" is a 2-character change, changing a password from "password" to "password2" is a 1-character change, and changing a password from "password" to "apassword" is a 9-character change.

number is the number of characters entered as an integer from 0 through 16.

[min-change-interval *days* **]**

Default: 1
Specifies the frequency that passwords can be changed (other than first login).
days is the minimum number of days that must pass before a user can change their password. It is an integer from 1 through 365.

Important: If the **no local-user password min-change-interval** command is used, users may change their password as often as desired which could allow them to circumvent the password history function.

[min-length *number* **]**

Default: 8
Specifies the minimum length allowed for user-defined password.
number is the minimum number of alphanumeric characters that the password must contain, entered as an integer from 3 through 32.

Usage

This command is used to set the property requirements for user-defined passwords and system behavior in relation to those passwords.
Information pertaining to user passwords, login failures, and password history are stored on the packet processing cards and in the software's Shared Configuration Task (SCT).

The system uses the information in the SCT for runtime operations such as determining password ages and determining if new passwords meet the criteria specified by this command.

Example

The following command configures a minimum password length requirement of *6* characters:

```
local-user password min-length 6
```

The following command configures the system to store the *4* most recently used passwords per user-account in the history list:

```
local-user password history length 4
```

local-user username

Adds or removes local-user administrative accounts.

Product

All

Privilege

Security Administrator, Administrator

Syntax

local-user username *name* **[authorization-level { administrator | inspector | operator | security-admin }] [ecs | noecs] [ftp | noftp] [timeout-min-absolute** *time* **] [timeoute-min-idle** *time* **] [no-lockout-login-failure] [no-lockout-password-aging] password** *password*

no local-user username *name*

no

Removes a previously configured user.

name

Specifies the name of the user as an alphanumeric string of 3 through 16 characters that is case sensitive.

[authorization-level { administrator | inspector | operator | security-admin }]

Default: Operator

Configures the authorization level for the user as one of the following:

- **administrator**: Administrator users have read-write privileges and can execute any command throughout the CLI except for a few security functions allowed only in the administrator mode. Administrators can configure or modify the system and are able to execute all system commands, including those available to the operator and inspector user. This level corresponds to the both the System Administrator and Application Administrator levels in the T1.276-2003.
- **inspector**: Inspector users are limited to a small number of read-only Exec Modecommands.The bulk of these are “show” commands giving the inspector the ability to view a variety of statistics and conditions. The Inspector cannot execute show configuration commands and do not have the privilege to enter the Config Mode.
- **operator**: Operator users have read-only privileges to a larger subset of the Exec Mode commands as depicted in the following figure. Operator users can execute all commands that are part of the inspector mode, plus some system monitoring, statistical, and fault management functions. Operators do not have the ability to enter the Config Mode.
- **security-admin**: Security Administrator users have read-write privileges and can execute any command throughout the CLI. Security Administrators can execute all system commands, including those available to the administrator, operator, and inspector users. This level corresponds to both the System Security Administrator and Application Security Administrator levels in T1.276-2003.

[ecs | noecs]

Specifies whether or not the user has access to Active Charging Service configuration parameters.

- **ecs**: The user has access.

- **noecs**: The user does not have access.

Default: **ecs**

[ftp | noftp]

Default: ftp
Specifies whether or not the user is allowed to access the system via the File Transfer Protocol (FTP) and/or the Secure File Transfer Protocol (SFTP).

- **ftp**: The user has access.
- **noftp**: The user does not have access.

[timeout-min-absolute *time* **]**

Default: 0
Specifics the maximum session time (in minutes) for this user. *time* is an integer from 0 through 525600. A value of "0" indicates no limit.

Important: This limit applies only to the user's CLI sessions.

[timeout-min-idle *time* **]**

Default: 0
Specifics the maximum idle time (in minutes) for this user. *time* is an integer from 0 through 525600. A value of "0" indicates no limit.

Important: This limit applies only to the user's CLI sessions.

[no-lockout-login-failure]

Default: Disabled
Specifies that this user will never be locked out due to login attempt failures.

[no-lockout-password-aging]

Default: Disabled
Specifies that this user will never be locked out due to the age of their password.

password *password*

Specifies the initial password for this user. *password* must an alphanumeric string of 6 through 32 characters that is case sensitive.

Important: The user is requested to change their password upon their first login.

Usage

The ability to configure administrative local-users is provided in support of the login security mechanisms specified in ANSI T1.276-2003.
Like administrative users configured at the context level, local-users can be assigned one of 4 security levels:

Local-User Level User	Context Level User

Local-User Level User	Context Level User
Security Administrator	Administrator
Administrator	Config-Administrator
Operator	Operator
Inspector	Inspector

Local-user configuration support is handled differently from that provided for administrative users configured at the context level.
Context-level administrative users rely on the system's AAA subsystems for validating user names and passwords during login. This is true for both administrative user accounts configured locally through a configuration file or on an external RADIUS server. Passwords for these user types are assigned once and are accessible in the configuration file.
Local-user account information (passwords, password history, lockout states, etc.) is maintained in non-volatile memory and in the software's Shared Configuration Task (SCT). This information is maintained in a separate file – not in configuration files used by the system. As such, the configured local-user accounts are not visible with the rest of the system configuration.
Local-user and context-level administrative accounts can be used in parallel.

Example

The following command configures a security-administrator level local-user administrative account for a user named *User672* that has FTP privileges, a temporary password of *abc123*, and that does not lockout due to either login attempt failures or password aging:

```
local-user username User672 authorization-level security-admin ftp no-
lockout-login-failure no-lockout-password-aging password abc123
```

The following command deletes a previously configured local-user administrative account called admin32:

```
no local-user username admin32
```

logging console

Enables the output of logged events to be displayed on the console terminal.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
logging console

no logging console
```

no

Disables the output of events to the console port.

Usage

Log console output to allow for offline review during system monitoring and/or trouble shooting.

logging disable

Enables/disables the logging of the specified event ID or range of IDs.

Product

All

Privilege

Security Administrator, Administrator

Syntax

logging disable eventid *id* **[to** *to_id* **]**

no logging disable eventid *id* **[to** *to_id* **]**

no

Indicates the event IDs specified are to be enabled for logging.

eventid *id*

Specifies the event for which no logging is to occur. *id* must be a integer from 1 through 100000.

to *to_id*

Specifies the end ID of the events when a range of event ID is to be disabled from being logged. *to_id* must be an integer from 1 through 100000. The *to_id* must be equal to or larger than the *id* specified.

Usage

Disable common events which may occur with a normal frequency are not of interest in monitoring the system for troubles.

Example

The following commands disables the logging of event ID 4580 and the range of events from 4500 through 4599, respectively.

```
logging disable eventid 4580 4580

logging disable eventid 4500 to 4599
```

The following enables the subset of disabled event IDs:

```
no logging disable eventid 4500 to 4549
```

logging display

Configures the level of detail for information to be logged.

Product

All

Privilege

Security Administrator, Administrator

Syntax

logging display event-verbosity *evt_level* **] [pdu-data** *format* **] [pdu-verbosity** *pdu_level* **]**

event-verbosity *evt_level*

Specifies the level of verboseness to use in logging of events as one of:

- min
- concise
- full

pdu-data *format*

Specifies output *format* for packet data units when logged as one of:

- **none**: outputs in raw format
- **hex**; displays out in hexadecimal format
- **hex-ascii**; displays output in hexadecimal and ASCII similar to a main-frame dump

pdu-verbosity *pdu_level*

Specifies the level of verboseness to use in logging of packet data units as an integer from 1 through 5, where 5 is the most detailed.

Usage

Tune the level of information to be logged so as to avoid flooding a log file with information which is not useful or critical.

Example

The following sets the logging display for events to the maximum.

```
logging display event-verbosity full
```

The following command sets the logging display level of detail for packet data units to level *3* and sets the output format to the main-frame style *hex-ascii*:

```
logging display pdu-data hex-ascii pdu-verbosity 3
```

logging filter

Configures the logging of events to be performed in real time for the specified facility.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
logging filter runtime facility facility level report_level [ critical-info | no-
critical-info ]
```

facility *facility*

Specifies the facility to modify the filtering of logged information. The following list displays the valid facilities for this command:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: AAA client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **aal2**: AAL2 protocol logging facility
- **acl-log**: Access Control List logging facility
- **acsctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: Active Charging Service (ACS) Manager facility
- **alarmctrl**: Alarm Controller facility
- **alcap**: ALCAP protocol logging facility
- **alcapmgr**: ALCAPMgr logging facility
- **all**: All facilities
- **asngwmgr**: ASN Gateway Manager facility
- **asnpcmgr**: ASN Paging Controller Manager facility
- **bfd**: BFD protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux-De-mux Manager logging facility
- **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
- **callhome**: Call home application logging facility

- **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
- **cli**: CLI logging facility
- **credit-control**: Credit Control facility
- **cscf**: IMS/MMD CSCF
- **cscfmgr**: SIP CSCF Manager facility
- **cscfttmgr**: SIP CSCFTT Manager facility
- **csp**: Card Slot Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: Content Service Selection (CSS) RADIUS Signaling facility
- **cx-diameter**: Cx Diameter Messages facility
- **dcardctrl**: IPSEC Daughter Card Controller logging facility
- **dcardmgr**: IPSEC Daughter Card Manager logging facility
- **demuxmgr**: Demux Manager API facility
- **dgmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol logging facility
- **dhcpv6**: DHCPv6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages facility
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting
- **diameter-auth**: Diameter Authentication
- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ACS Diameter signaling facility
- **diameter-hdd**: Diameter HDD Interface facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSEC Data Path facility
- **drvctrl**: Driver Controller facility
- **eap-ipsec**: EAP
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface facility
- **egtpc**: eGTP-C logging facility
- **egtpmgr**: eGTP manager logging facility
- **egtpu**: eGTP-U logging facility
- **epdg**: ePDG logging facility
- **evlog**: Event log facility

- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
- **fng**: FNG logging facility
- **gmm**:
  - For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
  - For 3G: Logs the access application layer (above the RANAP layer)
- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
- **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
- **gss-gcdr**: GTPP Storage Server GCDR facility
- **gtpc**: GTP-C protocol logging facility
- **gtpcmgr**: GTP-C protocol Manager logging facility
- **gtpp**: GTP-PRIME protocol logging facility
- **gtpu**: GTP-U protocol logging facility
- **gtpumgr**: GTPU Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages facility
- **gy-diameter**: Gy Diameter messages facility
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **hdctrl**: HD Controller logging facility
- **hnb-gw**: HNB-GW (3G Femto GW) logging facility
- **hnbmgr**: HNBMGR (3G Femto GW DemuxMgr) logging facility
- **hss-peer-service**: HSS Peer Service facility
- **igmp**: IGMP
- **ikev2**: IKEv2
- **ims-authorizatn**: IMS Authorization Service facility
- **ims-sh**: HSS SH Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **imsue**: IMSUE
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipms**: IPMS logging facility
- **ipsec**: IP Security logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ipsp**: IP Pool Sharing Protocol logging facility

- **kvstore**: KV Store facility
- **l2tp-control**: L2TP control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: LAGMGR logging facility
- **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
- **li**: Refer to the *Lawful Intercept Interface Reference* for a description of this command.
- **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
- **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
- **local-policy**: Local Policy Service facility
- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway manager logging facility
- **map**: MAP Protocol logging facility
- **megadiammgr**: Megadiameter Manager (SLF Service) logging facility
- **mme-app**: Mobility Management Entity Application logging facility
- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: Mobility Management Entity Demux Manager logging facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 logging facility
- **mpls**: MPLS protocol logging facility
- **mseg-app**: MSEG application logging facility
- **mseg-gtpc**: MSEG GTPC application logging facility
- **mseg-gtpu**: MSEG GTPU application logging facility
- **msegmgr**: MSEGMgr (MSEG DemuxMgr) logging facility
- **mtp2**: MTP2 Service logging facility
- **mtp3**: MTP3 Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **npuctrl**: Network Processor Unit Control facility
- **npumgr**: Network Processor Unit Manager facility
- **npumgr-acl**: NPUMGR ACL logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility
- **npumgr-fwd**: NPUMGR FWD logging facility

- **npumgr-init**: NPUMGR INIT logging facility
- **npumgr-port**: NPUMGR PORT logging facility
- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **ntfy-intf**: Notification Interface logging facility
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF protocol logging facility
- **ospfv3**: OSPFv3 protocol logging facility
- **p2p**: Peer-to-Peer Detection logging facility
- **pccmgr**: IPCF PCC Manager library
- **pdg**: PDG logging facility
- **pdgdmgr**: PDG Demux Manager logging facility
- **pdif**: PDIF logging facility
- **pgw**: PDN Gateway logging facility
- **phs**: Payload Header Suppression
- **phs-control**: PHS X1/X5 and X2/X6 Interface logging facility
- **phs-data**: PHS Data logging facility
- **phs-eapol**: PHS EAPOL logging facility
- **phsgwmgr**: PHS Gateway Manager facility
- **phspcmgr**: PHS Paging Controller Manager facility
- **pmm-app**: PMM application logging facility
- **ppp**: PPP link and packet facilities
- **pppoe**: PPPOE logging facility
- **push**: VPNMGR CDR push logging facility
- **radius-acct**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Rf Diameter messages facility
- **rip**: RIP logging facility (RIP is not supported at this time.)
- **rohc**: RObust Header Compression facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RUA (3G Femto GW - RUA messages) logging facility
- **s1ap**: S1AP Protocol logging facility

- **sccp:** SCCP Protocol logging connection-oriented messages between RANAP and TCAP layers.
- **sct**: Shared Configuration Task logging facility
- **sctp**: SCTP Protocol logging facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN 'glue' interfaces, e.g., between PMM, MAP,. GPRS-FSM, SMS.
- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN MBMS Bearer app (SMGR) logging facility
- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSNs System Components logging facility; used infrequently
- **sgsn-test**: SGSN Tests logging facility; used infrequently
- **sgtpcmgr**: SGSN GTPC Manager logging information exchange through SGTPC and the GGSN
- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages facility
- **sitmain**: System Initialization Task main logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
- **sndcp**: SNDCP Protocol logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF SPR Manager logging facility
- **srdb**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **sscfnni**: SSCFNNI Protocol logging facility
- **sscop**: SSCOP Protocol logging facility
- **ssh-ipsec**: SSH IP Security logging facility
- **ssl**: SSL (Secure socket layer messages) logging facility
- **stat**: Statistics logging facility
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **tcap**: TCAP Protocol logging facility
- **testctrl**: Test Controller logging facility

- **testmgr**: Test Manager logging facility
- **threshold**: threshold logging facility
- **ttg**: TTG logging facility
- **tucl**: TUCL logging facility
- **udr**: User detail record facility (used with the Charging Service)
- **user-data**: User data logging facility
- **user-l3tunnel**: User layer-3 tunnel logging facility
- **usertcp-stack**: User TCP Stack
- **vpn**: Virtual Private Network logging facility
- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6

level *report_level* **[critical-info | no-critical-info]**

level *report_level*: specifies the level of information to be logged, *report_level*, as one of:

- critical
- debug
- error
- info
- trace
- unusual
- warning

critical-info | **no-critical-info**: indicates if critical information is to be displayed or not. The keyword **critical-info** specifies that events with a category attribute of critical information are to be displayed. Examples of these types of events can be seen at bootup when system processes and tasks are being initiated. The **no-critical-info** keyword specifies that events with a category attribute of critical information are not to be displayed.

Usage

This command is useful when it is necessary to get real time output of events. Event output may be cached otherwise which may make it difficult to trouble shoot problems which do not allow the last cache of events to be output prior to system problems.

Caution: Issuing this command could negatively impact system performance depending on system loading, the log level, and/or the type of facility(ies) being logged.

Example

Set real time output for the point-to-point protocol facility and all facilities, respectively, to avoid logging of excessive information.

```
logging filter runtime facility ppp

logging filter runtime facility all level warning
```

logging monitor

Enables or disables the monitoring of a specified user.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] logging monitor {ipaddr *ip_address* **| msid** *ms_id* **| username user_name}**

no

Disables the monitoring of the user specified by the options given.

ipaddr *ip_address*

Specifies the IP address of the user for which the monitoring filter is to be set. *ip_address* must entered using IPv4 dotted-decimal notation.

msid *ms_id*

msid *ms_id*: specifies the mobile subscriber ID for which the monitoring filter is to be set. *ms_id* must be from 7 to 16 digits.
This keyword/option can be used to specify the Mobile Subscriber ISDN (MSISDN) for GGSN calls which enables logging based on MSISDN.

username *user_name*

username *user_name*: specifies a user for which the monitoring filter is to be set. *user_name* must refer to a previously configured user.

Usage

Monitor subscribers which have complaints of service availability or to monitor a test user for system verification.

Caution: Issuing this command could negatively impact system performance depending on the number of subscribers for which monitoring is performed and/or the amount of data they're passing.

Example

The following command enables the monitoring of user *user1* and mobile subscriber ID 4441235555, respectively.

```
logging monitor username user1

logging monitor msid 44441235555
```

The following disables the monitoring of user *user1*.

```
no logging monitor username user1
```

logging runtime

Enables events to be filtered and logged in real time.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
logging runtime buffer store { all-events | filtered-events-only }
```

buffer store { all-events | filtered-events-only }

Determines which logs are stored in internal logging daemon runtime buffer.

- **all-events**: Logging daemon runtime buffer stores all logs that come to it.
- **filtered-events-only**: Logging daemon runtime buffer stores only logs that pass the runtime filter.

Usage

Sets the filtering of logged information to log in real time.

Example

The following command enables storage of logs that pass the runtime filter:

```
logging runtime buffer store filtered-events-only
```

lte-policy

This command enters the LTE Policy Configuration Mode where LTE policy parameters can be configured.

Product

MME, S-GW

Privilege

Administrator

Syntax

lte-policy

Usage

Enters the LTE Policy Configuration Mode.
Entering this command results in the following prompt:
`[context_name]hostname(lte-policy)#`
LTE Policy Configuration Mode commands are defined in the *LTE Policy Configuration Mode Commands* chapter.

mediation-device

This command is obsolete. Even though the CLI accepts the command no function is performed.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] mediation-device mode { tcs }
```

mobile-services-edge-gateway

This command allows you to enter the MSEG Global Configuration Mode wherein the global Mobile Edge Service Gateway (MSEG) parameters can be configured.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

```
mobile-services-edge-gateway
```

Usage

Use this command to enter the MSEG Global Configuration Mode.
Also see the *MSEG Global Configuration Mode Commands* chapter.

network-overload-protection

This command configures an attach rate throttle mechanism to control the number of new connections (attaches or inter-SGSN RAUs), through the SGSN, on a per second basis.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

network-overload-protection sgsn-new-connections-per-second *#_new_connections* **action { drop | reject with cause { congestion | network failure } } [queue-size** *queue_size* **] [wait-time** *wait_time* **]**

default network-overload-protection sgsn-new-connections-per-second

default

Using **default** in the command, disables this attach rate throttle feature that provides network overload protection.

sgsn-new-connections-per-second *#_new_connections*

Define the number of new connections to be accepted per second.
#_new_connections: Must be an integer from 50 to 5000.

action

Specifies the action to be taken by the SGSN when the attach rate exceeds the configured limit on the number of attaches. Select one of the following actions:

- **drop:** Drop the new connection request.
- **reject-with-cause:** Reject the new connection request. Include one of the following as the cause in the reject message:
- **congestion**
- **network failure**

queue-size *queue_size*

Defines the maximum size of the pacing queue used for buffering the packets. If configured, the queue-size should be greater than or equal to the *#_new_connections* value and less than or equal to the optimal value (the *wait_time* * *#_new_connections*). This validation is done in the CLI.
queue_size Must be an integer from 250 to 25000.
Default: unconfigured. The default value is the *#_new_connections* * *wait-time*. This will be the optimal value.

wait-time *wait_time*

Defines the maximum life-time (number of seconds) of the packets in the queue beyond which the packets are considered to be “stale”.
wait_time Must be an integer from 1 to 15

Default: 5

Usage

Use this command to configure the rate at which the SGSN must process new connection requests. The rate is the number of new connections to be accepted per second.
With basic network overload protection, the incoming new connection rate is higher than this configured rate. When this occurs, all of the new connection requests cannot be processed. This command can also be used to configure the action to be taken when the rate limit is exceeded. The new connection requests, which cannot be processed, can be either dropped or rejected with a specific reject cause.
The SGSN's *optimized* network overload protection performs attach-rate throttling to avoid overloading Gr, Gn and Gf interfaces. This is enabled with **queue-size** and **wait-time** keywords so that the IMSIMgr throttles the attach rate to values configured with these keywords.
If the SGSN receives more than the configured number of attaches in a second, then the attaches are buffered in the pacing queue and requests are only dropped when the buffer overflows due to high incoming attach rate. Messages in the queue are processed (FIFO) until they age-out when the queued message's lifetime crosses the configured wait-time. The wait-time and the attach rate decide the optimal size of the queue.
Counters for this feature are available in the **show gmm-sm statistics** command display in the Network Overload Protection portion of the table.

Example

Configure the throttle rate or limit to 2500 attaches per second and to drop all requests if the limit is exceeded.

```
network-overload-protection sgsn-new-connections-per-second 2500 action
drop
```

Disables the network-overload protection feature and set the default queue size to 1000 and the wait time to 5 seconds:

```
default network-overload-protection sgsn-new-connections-per-second
```

Set the attach rate to 500 per second, the action to drop, the wait time to 5 seconds, and the queue size to be calculated (as follows: *wait_time* * *#_new_connections* - i.e., 2500)

```
network-overload-protection sgsn-new-connections-per-second 500action
drop wait-time 5
```

network-service-entity

This command creates a new instance of an SGSN network service entity (NSE) for either the IP environment or the Frame Relay environment.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] network-service-entity (ip-local | peer-nsei *peer_nsei_number* **frame-relay)**

no

Deletes the network service entity definition from the system configuration.

ip-local

Configures the local endpoint for NS/IP and enters the NSE-IP configuration mode. The prompt will change to:

```
[local]<hostname>(nse-ip-local)#
```

peer-nsei *peer_nsei_number* **frame-relay**

Configures a peer NSE with frame relay connectivity. This set of keywords also provides access to the NSE-FR Configuration mode. The prompt will change to:

```
[local]<hostname>(nse-fr-peer-nsei-<peer_nsei_number>)#
```

Usage

Use this command to access the configuration modes for either the IP or Frame Relay network service entities.

Example

Enter the NSE for a Frame Relay configuration instance identified as 4554:

```
network-service-entity peer-nsei 4554 frame-relay
```

network-service-entity ip

This command has been deprecated. See the replacement command network-service-entity .

ntp

Enters the network timing protocol configuration mode or disables the use of NTP on the system.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ntp

no ntp

no

Disables the use of NTP for clock synchronization. When omitted, the NTP client support is enabled on the chassis.

Important: If the use of NTP is disabled the system clock may drift over a period of time. This may require manual updates to the system clock to synchronize the clock with other network elements.

Usage

Used when it is necessary to configure NTP settings.

Example

The following command enters the NTP configuration mode:

```
ntp
```

The following disables the use of the network timing protocol for system clock synchronization.

```
no ntp
```

operator-policy

This command creates an operator policy and enters the operator policy configuration mode. Commands for configuration of the policies are available in the *Operator Policy Configuration Mode Commands* chapter.

Product

MME, SGSN, S-GW

Privilege

Security Administrator, Administrator

Syntax

```
operator-policy ( default | name policy_name } [ -noconfirm ]

no operator-policy ( default | name policy_name }
```

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

no

Removes the specified operator policy from the system configuration.

default

default, in this case, is the *name* of a specific operator policy. This default policy is used when no other defined operator policy matches the incoming IMSI.

Important: You should configure this default operator policy to be it available to handle IMSIs that are not matched with other defined policies.

name *policy_name*

Specifies the unique name of an operator policy. *policy_name* is entered as an alphanumeric string of 1 through 64 characters.

Usage

Use this command to create an operator policy and to enter the operator policy configuration mode to define or modify policies.

An operator policy associates APNs, APN profiles, IMEI ranges, IMEI profiles, an APN remap table and a call-control profile to ranges of IMSIs. These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. In this manner, an operator policy manages the application of rules governing the services, facilities and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements such as DNS servers and HLRs.

The system supports up to 1,000 operator policies, including the *default* operator policy.

Important: An operator policy is **the** key element of the Operator Policy feature. After defining an instance of an operator policy, you must go to the SGSN Global Configuration Mode (from the Global Configuration mode) to define the IMSI range(s). This requirement does not hold if you are using a *default* operator policy.

To see what operator policies have already been created, return to the Exec mode and enter the **`show operator-policy all`** command.

Example

The following command accesses the default operator policy and enters the operator policy configuration mode to view or modify the specified policy:

```
operator-policy default
```

orbem

Enters the Object Request Broker Element Manager (ORBEM) Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

orbem

Usage

Set the configuration mode to allow modification of the ORBEM configuration data.

pac-standby-priority

This command has been renamed to **`card-standby-priority`**. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.

port atm

Identifies a physical port on a line card that supports ATM signaling and then enters the configuration mode for the specific interface-type. For the commands to configure the port interface, see the CLI chapter ATM Port Configuration Mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

port atm *slot/port*

atm

Indicates the port identified is an ATM interface port.

slot/port

To determine valid ATM slot and port numbers, use the Exec mode's command **show port table**
slot: Identifies the chassis slot holding the line card that supplies ATM ports. The slot ID number can be an integer from 17 through 48.
port: Identifies the physical port that is to be configured to support ATM signaling. The ID number can be an integer from 1 through 4.

Usage

Change the current configuration mode to Ethernet Port Configuration mode.

Important: This command is not supported on all platforms.

Example

The following enters the ATM port configuration mode for ATM port 1 on the card in slot 19:

```
port atm 19/1
```

port bits

Enters the Building Integrated Timing Supply (BITS) port configuration mode by identifying the BITS port on the active or standby SPIO.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

port bits *slot/port*

bits

Identifies the BITS port.

slot/port

slot: Identifies the chassis slot holding the SPIO. The slot ID can be either 24 (active SPIO) or 25 (standby SPIO).
port: Identifies the BITS port on the SPIO. The port ID number must be 4.

Usage

Change the current configuration mode to BITS port configuration mode.

Important: This command is not supported on all platforms.

Example

The following enters the BITS port configuration mode for the active SPIO:

```
port bits 24/4
```

port channelized

Identifies a physical port on a Channelized Line Card (CLC) that supports Frame Relay signaling and creates a Frame Relay interface. This command enters the configuration mode for the commands that configure the Frame Relay interface and the channelized port interface. For additional information, see the *Channelized Port Configuration Mode Commands* chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

port channelized *slot/port*

channelized

Selects the channelized frame relay interface for the selected line card and port.

slot/port

To determine valid slots and port numbers, use the Exec mode's command **show port table** to find the channelized line card**.**
slot: Identifies the chassis slot holding the Channelized Line Card that sources Frame Relay ports. The slot ID number can be an integer from 17 through 48.
port: Identifies the physical port that is to be configured to support Frame Relay signaling. The ID number can only be 1.

Usage

Change the current configuration mode to Channelized Port configuration mode.

Example

The following enters the Channelized port configuration mode for port 1 on the card in slot 20:

```
port channelized 20/1
```

port ethernet

Enters the Ethernet Port Configuration mode for the identified port.

Product

All

Privilege

Security Administrator, Administrator

Syntax

port ethernet *slot/port*

ethernet

Indicates the port identified is an Ethernet interface port.

slot/port

Specifies the port for which Ethernet Port Configuration mode is being entered. The slot and port must refer to an installed card and port.

Usage

Change the current configuration mode to Ethernet Port Configuration mode.

Example

The following command enters the Ethernet Port Configuration mode for ethernet port 1 in slot 17:

```
port ethernet 17/1
```

port mac-address virtual-base-address

This command defines a block of 256 consecutive media access control (MAC) addresses and enables virtual MAC addressing for Ethernet line card ports. Not available for the XT2 platform.

Product

All

Privilege

Security Administrator, Administrator

Syntax

port mac-address virtual-base-address *MAC_Address*

no port mac-address virtual-base-address

no

Disables virtual MAC addressing for Ethernet line card ports. The block of virtual MAC addresses is not saved.

MAC_Address

Specifies the beginning address of a block of 256 MAC addresses that are used for virtual MAC addressing.

Usage

Use this command to disregard the MAC addresses assigned and stored in card firmware and assign MAC addresses for all Ethernet ports from the specified block of virtual MAC addresses. This command does not affect the MAC addresses on SPIO cards.
There are 65536 MAC addresses (00:05:47:FF:00:00 - 00:05:47:FF:FF:FF) reserved for use by customers. This range allows for the creation of 256 address blocks each containing 256 MAC addresses (for example, 00:05:47:FF:00:00, 00:05:47:FF:01:00, 00:05:47:FF:02:00, 00:05:47:FF:03:00, 00:05:47:FF:04:00, etc.).

Caution: This configuration requires the configuration of a valid block of unique MAC addresses that are not used anywhere else. Use of non-unique MAC addresses can degrade and impair the operation of your network.

Important: This command is not supported on all platforms.

Example

To enable virtual MAC addressing for Ethernet ports on all Ethernet line cards in the system using a block of MAC addresses starting at *00:05:47:FF:00:00*, enter the following command:

```
port mac-address virtual-base-address 00:05:47:FF:00:00
```

port rs232

Enters the RS-232 Port Configuration mode for the RS-232 console port on the specified SPIO card. Not available on the XT2 platform.

Product

All

Privilege

Security Administrator, Administrator

Syntax

port rs232 *slot* **3**

rs232

Indicates the port identified is an RS-232 port on a SPIO card.

slot **3**

Specifies the slot of the SPIO for which RS-232 Port Configuration mode is being entered. The slot must refer to an installed SPIO card. The specified port must always be 3 for an RS-232 port.
The value for *slot* must be either 24 or 25.

Usage

Change the current configuration mode to RS-232 Port Configuration mode.

Example

The following command enters the RS-232 Port Configuration mode for the SPIO in slot 24;

```
port rs232 24 3
```

profile-id-qci-mapping

Creates a Qos Class-Identifier-Radio Access Network (QCI-RAN) ID mapping table or specifies an existing table and enters the QCI Mapping Configuration mode for the system.

Product

HSGW

Privilege

Administrator

Syntax

[no] profile-id-qci-mapping *name* **[-noconfrm]**

no

Removes the specified mapping table from the system

name

Creates a new or enters an existing mapping table configuration. *name* must be an alphanumeric string of 1 through 63 alphanumeric.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Enters the QCI-RAN ID mapping configuration mode for an existing table or for a newly defined table. This command is also used to remove an existing table.
Entering this command results in the following prompt:

```
[context_name]hostname(config-hsgw-association-table)#
```

QCI Mapping Configuration Mode commands are defined in the *QCI Mapping Configuration Mode Commands* chapter.
Use this command when configuring the HSGW eHRPD component.

Important: This command creates a mapping table available to any HSGW context configured on the system.

Example

The following command enters the existing QCI mapping configuration mode (or creates it if it doesn't already exist) for a mapping table named *qci_table1*:

```
profile-id-qci-mapping qci_table1
```

The following command will remove *qci_table1* from the system:

```
no profile-id-qci-mapping qci_table1
```

ps-network

This command creates/removes an HNB-PS network configuration instance for Femto UMTS access over Iu-PS/Iu-Flex interface between Home NodeB Gateway (HNB-GW) service and PS networks elements; i.e. SGSN. This command also configures an existing HNB-CS network instance and enters the HNB-CS Network Configuration mode on a system.

Product

HNB-GW

Privilege

Administrator

Syntax

```
[ no ] ps-network ps_instance [ -noconfirm ]

no ps-network ps_instance
```

no

Removes the specified HNB-PS network instance from the system.

Caution: Removing the HNB-PS network instance is a disruptive operation and it will affect all UEs accessing SGSN(s) in specific PS core network through the HNB-GW service.

WARNING: If any HNB-PS Network instance is removed from system all parameters configured in that mode will be deleted and Iu-PS/Iu-Flex interface will be disabled.

ps_instance

Specifies the name of the Packet Switched Core Networks instance which needs to be associated with HNB Radio Network PLMN in HNB RN-PLMN configuration mode. If *ps_instance* does not refer to an existing HNB-PS instance, the new HNB-PS network instance is created.
ps_instance must be an alphanumeric string of 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to enter the HNB-PS Network Configuration mode for an existing PS network instance or for a newly defined HNB-PS network instance. This command is also used to remove an existing HNB-PS network instance.
This configuration enables the Iu-PS/Iu-Flex interface on HNB-GW service with CS core network elements; i.e. MSC/VLR.
A maximum of 1 HNB-PS networks instance which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

Caution: This is a critical configuration. The HNBs can not access SGSNs in PS core network without this configuration. Any change to this configuration would lead to disruption in HNB access to PS core network.

Entering this command results in the following prompt:

```
[context_name]hostname(config-ps-network)#
```

The various parameters available for configuration of an HNB-PS network instance are defined in the *HNB-PS Network Configuration Mode Commands* chapter.

Example

The following command enters the existing HNB-PS Network configuration mode (or creates it if it doesn't already exist) for the instance named *hnb-ps1*:

```
ps-network hnb-ps1
```

The following command will remove HNB-PS network instance *hnb-ps1* from the system without any prompt to user:

```
no ps-network hnb-ps1
```

qci-qos-mapping

Global QCI-QoS mapping tables are used to map QoS Class Identifier (QCI) values to appropriate Quality of Service (QoS) parameters.

Product

HSGW, P-GW, S-GW

Privilege

Administrator

Syntax

qci-qos-mapping *name* **[-noconfirm]**

no

Removes the specified mapping configuration from the system

name

Creates a new or enters an existing mapping configuration. *name* must be an alphanumeric string of 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Enter the QCI-QoS mapping configuration mode for an existing table or for a newly defined table. This command is also used to remove an existing table.
Entering this command results in the following prompt:

```
[context_name]hostname(config-qci-qos-mapping)#
```

QCI - QoS Mapping Configuration Mode commands are defined in the *QCI - QoS Mapping Configuration Mode Commands* chapter.
Use this command when configuring the following eHRPD component: HSGW, P-GW, S-GW.

Important: This command creates a mapping configuration available to any HSGW, P-GW, S-GW context configured on the system.

Example

The following command enters the existing QCI - QoS mapping configuration mode (or creates it if it doesn't already exist) for a mapping configuration named *qci-qos3*:

```
qci-qos-mapping qci-qos3
```

qos npu inter-subscriber traffic bandwidth

Configures NPU QoS bandwidth allocations for the system.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

qos npu inter-subscriber traffic bandwidth gold *percent* **silver** *percent* **bronze** *percent* **best-effort** *percent*

no qos npu inter-subscriber traffic bandwidth

no

Removes a previous bandwidth allocation.

gold *percent*

Default: 10%
Specifies the maximum percentage of bandwidth to be allocated to the gold queue priority.
percent can be configured to an integer from 0 through 100.

silver *percent*

Default: 20%
Specifies the maximum percentage of bandwidth to be allocated to the silver queue priority.
percent can be configured to an integer from 0 through 100.

bronze *percent*

Default: 30%
Specifies the maximum percentage of bandwidth to be allocated to the bronze queue priority.
percent can be configured to an integer from 0 through 100.

best-effort *percent*

Default: 40%
Specifies the maximum percentage of bandwidth to be allocated to the best-effort queue priority.
percent can be configured to an integer from 0 through 100.

Usage

The bandwidth of a subscriber queue is maintained by rate limiting functions which implement packet-rate limiting at the first level and bit-rate limiting at the next level.
The packet-rate limit of a queue is defined by the number of packets-per-second (PPS) permitted for queuing. Before queuing a packet on a subscriber queue, the NPU ensures that the packet falls within the limit. If the packet to be queued exceeds the packet rate limit, it is dropped.
Each subscriber queue is configured with a bit rate limit, measured in megabits-per-second (Mbps), referred to as CP-BPS (bit-per-second to CP). The CP-BPS is available as the total bandwidth for the subscriber traffic

that a CP can sustain. Each subscriber queue receives an allocation of a certain percentage of the CP-BPS. The following maximum CP-BPS values are supported:

- Lead CP (CP0) = 128 Mbps
- Remaining CPs (CP1, CP2, CP3) = 256 Mbps

For additional information on the NPU QoS functionality, refer to the System Administration and Configuration Guide.

Important: This functionality is not supported for use with the PDSN at this time.

Example

The following command configures bandwidth allocations of 20, 30, 40, and 50% for the gold, silver, bronze, and best-effort queues respectively:

```
qos npu inter-subscriber traffic bandwidth gold 20 silver 30 bronze 40
best-effort 50
```

Upon executing this command, the priority queues will have the following packet processing card CP bandwidth allocations based on the maximum CP bandwidth specifications:

Priority	Lead CP (CP 0) Bandwidth (Mbps)	CP 1 through CP 3 Bandwidth (Mbps)
Gold	25.6	51.2
Silver	38.4	76.8
Bronze	51.2	102.4
Best-effort	64	128

qos npu inter-subscriber traffic bandwidth-sharing

Configures NPU QoS bandwidth sharing properties for the system.

Product

PDSN, GGSN

Privilege

Administrator

Syntax

qos npu inter-subscriber traffic bandwidth-sharing { { enable | disable } { all | slot *slot_num* **cpu** *cpu_num* **} }**

enable

Enables bandwidth sharing for the specified criteria.

disable

Disables bandwidth sharing for the specified criteria.

all

Specifies that the bandwidth action is to be applied to all packet processing cards and every CPU on each packet processing card.

slot *slot_num*

Specifies that the bandwidth action is to be applied to a packet processing card in a specific chassis slot number.
slot_num is the slot in which a packet processing card is installed. These cards can be installed in slots 1 through 8, and/or 10 through 16.

cpu *cpu_num*

Specifies a specific control processor (CP) on a packet processing card for which to perform the bandwidth action.
cpu_num is an integer value from 0 to 3. 0 represents the lead CP.

Usage

The available bandwidth of a subscriber queue can be shared equally among the other subscriber queues. Any unutilized bandwidth of a queue can be shared with the other queues equally. For example, if only one DSCP is configured and it is mapped to best-effort, that DSCP would get the bandwidth allocated to the best-effort in addition to the rest of the bandwidth allocated to the gold, silver, and bronze.
By default, the system enables sharing for all packet processing cards and their CPs.
For additional information on the NPU QoS functionality, refer to the *System Administration Guide*.

Important: This functionality is not supported for use with the PDSN at this time.

Example

The following command disables bandwidth sharing for the fourth CP (CP 3) on a packet processing card installed in chassis slot 3:

```
qos npu inter-subscriber traffic bandwidth-sharing disable slot 4 cpu 3
```

qos npu inter-subscriber traffic priority

Configures the DSCP-to-Priority assignments for the system.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

qos npu inter-subscriber traffic priority { best-effort | bronze | gold | silver } assigned-to dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | *dscp_num* } }

no qos npu inter-subscriber traffic priority [assigned-to dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef }]

best-effort

Specifies the best-effort queue priority.

bronze

Specifies the bronze queue priority.

gold

Specifies the gold queue priority.

silver

Specifies the silver queue priority.

af*XX*

Assigns the Assured Forwarding *XX* PHB (per-hop behavior) DSCP.
Each Assured Forwarding PHB has a corresponding DSCP value as follows:

- af11 through af13: DSCP values 5 through 7 respectively
- af21 through af23: DSCP values 9 through 11 respectively
- af31 through af33: DSCP values 13 through 15 respectively
- af41 through af43: DSCP values 17 through 19 respectively

be

Assigns the Best Effort forwarding PHB which has a corresponding DSCP value of 0.

ef

Assigns the Expedited Forwarding PHB which has a corresponding DSCP value of 23.

dscp_num

Specifies a specific DSCP value as an integer from 0 through 31.

Usage

The differentiated services (DS) field of a packet contains six bits (0-5) that represent the differentiated service code point (DSCP) value.
Five of the bits (1-5) represent the DSCP. Therefore, up to 32 (25) DSCPs can be assigned to the various priorities. By default, they're all assigned to the lowest priority (best-effort).
For additional information on the NPU QoS functionality, refer to the *System Administration Guide*.

Important: This functionality is not supported for use with the PDSN at this time.

Example

The following command maps the ef DSCP to the gold priority queue:

```
qos npu inter-subscriber traffic priority gold assigned-to dscp ef
```

ran-peer-map

Creates a Radio Access Network (RAN) Peer Map and enters the RAN Peer Map Configuration Mode.

Product

ASN-GW, PHS

Privilege

Administrator

Syntax

[no] ran-peer-map *name* **[-noconfirm]**

no

Removes the RAN Peer Map from the system.

name

Specifies the name of the RAN Peer Map. *name* must be an alphanumeric string of 1 through 31 characters.

Usage

Use this command to create a new RAN Peer Map or edit an existing one. RAN peer maps reconcile base station MAC addresses received in R6 protocol messages to the base station's IP address.
Entering this command results in the following prompt:

```
[context_name]hostname(config-ran-peer-map)#
```

RAN Peer Map Configuration Mode commands are defined in the ASN RAN Peer Map Configuration Mode Commands chapter in this guide.

Example

The following command creates a RAN peer map named *ran12*:

```
ran-peer-map ran12
```

require active-charging

This command enables/disables Active Charging Service (ACS) with or without the Category-based Content Filtering application.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
require active-charging [ isolated-mode ] [ content-filtering category [ static-and-dynamic ] ] [ optimized-mode ]

no require active-charging
```

no

Disables ACS on the system.

isolated-mode

Enables ACS and separates ACS-related resources from other sub-system resource sharing.

Important: In 8.1 and later releases, this keyword is not supported.

optimized-mode

Enables ACS in Optimized mode, wherein ACS functionality is managed by SessMgrs.

Important: In 8.0 and earlier releases and in 9.0 and later releases, this keyword is not supported.

Important: In Release 8.1, ACS must be configured in the Optimized mode.

Important: In Release 8.1, if the active-charging mode is changed from the default (non-optimized) mode to the Optimized mode, or vice-versa, the system must be rebooted for the change to take effect.

Important: In Release 8.3, this keyword is obsolete. With or without this keyword ACS is always enabled in the Optimized mode.

Use the **require active-charging** command to enable ACS in the non-optimized mode. Wherein, ACS Managers will spawn to support ACS.
Use the **require active-charging optimized-mode** command to enable ACS in the Optimized mode. Wherein, ACS is enabled as part of Session Managers.

content-filtering category [static-and-dynamic]

Enables the Category-based Content Filtering application with ACS support and creates the necessary Static Rating Database (SRDB) tasks to utilize the internal database of static/dynamic URLs.
For Dynamic Content Filtering support, the **static-and-dynamic** keyword must be configured to specify that the Dynamic Rater Package (model and feature files) must be distributed to rating modules on startup, recovery, etc. If not configured, by default, the static-only mode is enabled.

Usage

Use this command to enable/disable ACS with or without Category-based Content Filtering application on the chassis.

Important: This command triggers the resource subsystem to switch to ACS-enabled mode and start ACS-related tasks. This CLI command must be configured before any services are configured, so that the resource subsystem can appropriately reserve adequate memory for the ACS-related tasks. After configuring this command, the configuration must be saved and the system rebooted in order to allocate the resources for ACS upon system startup.

In 8.0 and 8.1 releases, this command must be configured before configuring any services. This is to ensure that the resource subsystem can appropriately reserve adequate memory for ACS Manager tasks. If this command is configured after all the Session Manager tasks are already active, the ACS Manager tasks will not be started even if additional cards are added to the chassis—instead, the chassis must be rebooted.

Example

In Release 8.0, the following command enables resource subsystem to configure ACS in isolated mode:

```
require active-charging isoated-mode
```

In Release 8.1, the following command enables ACS in Optimized mode:

```
require active-charging optimized-mode
```

In Release 8.3, the following command enables ACS in Optimized mode:

```
require active-charging
```

require cipher ssl resource-percentage

Assigns the 8 processing cores on the PSC2 card and splits the hardware acceleration resources between SSL protocol and IPSec protocol processing.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Syntax

require cipher ssl resource-percentage *percentage_value*

default require cipher ssl resource-percentage

percentage_value

The system converts the specified resource percentage value to the nearest number of processing cores assigned to SSL processing. The system assigns the remaining processing cores to IPSec processing. This value can be within the range of 0 to 100.
For example, if 20% of the hardware acceleration resources are assigned to SSL processing, the system translates this value to INT((20*8+50)/100) = 2 processing cores assigned to SSL processing, and (8-2) = 6 processing cores assigned to IPSec processing.

default

Sets the default percentage value to 0%, assigning all 8 processing cores to IPSec processing.

Usage

Use this command to split the 8 processing cores on the PSC2 card between SSL protocol and IPSec protocol processing.

Example

The following command assigns 20% of the hardware acceleration resources on the PSC2 card (2 processing cores) to SSL processing, and 80% of the hardware acceleration resources (6 processing cores) to IPSec processing:

```
require cipher ssl resource-percentage 20
```

require demux card

This command enables or disables the demux capabilities.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] require demux card
```

default

Disables the demux capabilities on the card.

no

Disables the demux capabilities on the card.

Usage

Use this command configure the system to allow session recovery task placement scheme when session recovery is off.

Important: This command is not supported on all platforms.

Example

The following command enables demux capabilities:

```
require demux card
```

require detailed-rohc-stats

Enables or disables context-specific Robust Header Compression (RoHC) statistics.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ no ] require detailed-rohc-stats
```

no

Disables require detailed-rohc-stats. This is the default condition.

Usage

Enables context-specific statistics for RoHC calls.

Example

Enter the following command to enable context specific stats for RoHC calls:

```
require detailed-rohc-stats
```

require diameter-proxy

This command enables or disables Diameter Proxy mode.

Default: no require diameter-proxy

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
require diameter-proxy { master-slave | multiple | single }

no require diameter-proxy
```

no

Disables Diameter Proxy mode.

master-slave

Sets the Diameter-Proxy to Master-Slave mode.
In Master-slave mode, multiple Diameter proxies run on system, one on each packet processing card where one of them acts as Master and other Diameter proxies act as Slave.
In such mode the Master relays the traffic from an incoming connection to a specific Slave Diameter proxy.

multiple

To configure one Diameter proxy for each active packet processing card.

single

To configure one Diameter proxy for the entire chassis.

Usage

When the Diameter Proxy mode is enabled, each proxy process is a Diameter host, instead of requiring every Diameter application user (such as, every ACSMgr and/or every SessMgr, depending on the application) to be a host.
In Master-slave mode, multiple Diameter proxies runs on system, one on each packet processing card where one of them acts as Master and other Diameter proxies act as Slave.
In such mode Master relays the traffic from an incoming connection to a specific Slave Diameter proxy.

Example

To configure a Diameter proxy for each active packet processing card, enter the following command:

```
require diameter-proxy multiple
```

To configure a single Diameter proxy for the entire chassis, enter the following command:

```
require diameter-proxy single
```

require ecs credit-control subscriber-mode

This command configures the Diameter Credit-Control Application (DCCA) to work in per subscriber-PDN level Gy mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] require ecs credit-control subscriber-mode
```

no

Creates DCCA/Gy sessions per bearer/PDP-context.

Usage

This command is applicable to all products using the Gy interface. Use this command to configure DCCA/Gy to work in per subscriber-PDN level Gy mode, wherein one Diameter session is created per subscriber PDN rather than per bearer, and only one DCCA/Gy session is created for multi-bearer PDNs.
If this command is not configured, or the **no require ecs credit-control subscriber-mode** command is configured, DCCA/Gy sessions are created per bearer/PDP-context, and as a result when there are multiple PDP contexts or multiple bearers in a PDN as many DCCA/Gy sessions are created.

Important: This command will take effect only when the system is booted/rebooted. When configured after the system comes up, the command will be accepted but will not be applied until after the system is rebooted with the saved configuration.

Important: This command is independent of the **require active-charging** command. The **ecs** keyword in this command is license dependent.

require session recovery

Enables session recovery when hardware or software fault occurs within system.

Product

PDSN, GGSN, SGSN, HA, LNS, ASN-GW, PDIF, PDG/TTG, MME

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] require session recovery
```

no

Disables session recovery feature after configuration file is saved and system is restarted.

Usage

When this feature is enabled, the system attempts to recover any home agent-based Mobile IP sessions that would normally be lost due to a hardware or software fault within the system.
This functionality is available for the following call types:

- ASN-GW services supporting simple IP, Mobile IP, and Proxy Mobile IP
- PDSN services supporting simple IP, Mobile IP, and Proxy Mobile IP
- HA services supporting Mobile IP and/or Proxy Mobile IP session types with or without per-user Layer 3 tunnels
- GGSN services for IPv4 and PPP PDP contexts
- SGSN services for all attached and/or activated subscribers
- LNS session types
- PDIF services supporting Simple-IP, Mobile-IP and Proxy Mobile-P
- MME services

The default setting for this command is disabled.
The **no** option of this command disables this feature.
This command only works when the Session Recovery feature is enabled through a valid Session and Feature Use License Key.

Important: After entering this command, you must restart the system for the command takes effect. Remember to save the configuration file before issuing the **reload** command.

reveal disabled commands

Enables the input of commands for features that do not have license keys installed. The output of the command **show cli** indicates when this is enabled. This command effects all future CLI sessions. This is disabled by default.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] reveal disabled commands

no

Do not show disabled commands.

Usage

When this is enabled and a disabled command is entered, a message is displayed that informs you that the required feature is not enabled and also lists the name of the feature that you need to support the command. When this is disabled and a disabled command is entered, the CLI does not acknowledge the existence of the command and displays a message that the keyword is unrecognized.

Example

Set the CLI to accept disabled commands and display the required feature for all future CLI sessions with the following command:

```
reveal disabled commands
```

Set the CLI to reject disabled commands and return an error message for all future CLI sessions:

```
no reveal disabled commands
```

rohc-profile

This command allows you to create an RoHC (Robust Header Compression) profile and enter the RoHC Profile Configuration Mode. This mode is used to configure RoHC Compressor and Decompressor parameters. RoHC profiles can then be assigned to specific subscriber sessions when RoHC header compression is configured.

Product

HSGW, PDSN

Privilege

Security Administrator, Administrator

Syntax

rohc-profile profile-name *name* **[-noconfirm] [common-options | compression-options | decompression-options]**

no rohc-profile profile-name *name*

common-options

Configures common parameters for compressor and decompressor.

compression-options

Configures ROHC compression options.

decompression-options

Configures ROHC decompression options.

no

Remove the specified RoHC profile.

name

The name of the RoHC profile to create or remove. *name* must be an alphanumeric string of 1 through 63 characters.

-noconfirm

Do not prompt for additional verification when executing this command.

Usage

Use this command to enter the RoHC Profile Configuration mode.
Entering this command results in the following prompt:

```
[context_name]host(config-rohcprofile-<profile_name>)#
```

RoHC Profile Configuration Mode commands are defined in the *RoHC Profile Configuration Mode Commands* chapter.

Example

Enter the following command to create an RoHC profile named *HomeUsers* and enter the RoHC Configuration mode without prompting for verification:

```
rohc-profile profile-name HomeUsers
```

The following command removes the RoHC profile named *HomeUsers*:

```
no rohc-profile profile-name HomeUsers
```

sccp-network

This command creates or removes a Signaling Connection Control Part (SCCP) network instance which is used to define the SS7 end-to-end routing in a UMTS network. As well, this command enters the SCCP network configuration mode. The SGSN supports up to 12 SCCP network instances at one time.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

sccp-network *sccp_net_id* **[-noconfirm]**

no sccp-network *sccp_net_id*

no

Remove the SCCP network configuration with the specified index number from the system configuration.

sccp_net_id

This number identifies a specific SCCP network configuration.
sccp_net_id: must be an integer from 1 through 12.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create or modify an SCCP network and enter the SCCP network configuration mode. The SCCP network is not a standard SS7 or UMTS concept - this concept is specific to this platform.
For details about the commands and parameters needed to create and edit the SCCP Network configuration, check the *SCCP Network Configuration Mode* chapter.

Example

The following command creates an SCCP network with the index number of *1*:

```
sccp-network 1
```

The following command creates an SCCP network with the index number of *2* to associate with HNB-GW service for HNB access network users without any prompt.:

```
sccp-network 2 -noconfirm
```

sctp-parameter-template

This command allows you to create an SCTP parameter template and enter the SCTP Parameter Template Configuration Mode. This mode is used to configure parameters for SCTP associations.

Product

MME

Privilege

Administrator

Syntax

[no] sctp-param-template *name*

no

Removes the specified SCTP parameter template from the system.

name

Specifies the name of the SCTP parameter template being created or accessed. *name* must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to enter the SCTP Parameter Template Configuration mode.
Entering this command results in the following prompt:

```
[context_name]host(sctp-param-template)#
```

SCTP Parameter Template Configuration Mode commands are defined in the *SCTP Parameter Template Configuration Mode Commands* chapter.

Example

The following command creates a new SCTP parameter template or enters an existing template named *sctp-tmpl2*:

```
sctp-param-template sctp-tmpl2
```

session trace

This command configures the type of network elements, file transfer protocol, and Trace collection entity mode to be used for the transportation of trace files collected for the subscriber session tracing on the UMTS/EPC network element(s) along with network connection parameters and timers.

Product

GGSN, MME, P-GW, S-GW

Privilege

Administrator

Syntax

session trace network-element { all | mme | pgw | sgw | ggsn } [collection-timer *sec* **] [tce-mode { none | push transport sftp path** *string* **username** *name* **{ encrypted password** *enc_pw* **| password** *password* **} }]**

no session trace network-element { all | mme | pgw | sgw | ggsn }

---

no

Removes the entire session trace configuration from the system or a specific network element trace configuration.

---

network-element { all | mme | pgw | sgw | ggsn }

Identifies the type of service to the session trace application in order to determine the applicable interfaces.
all: Specifies that all network elements and their associated interfaces are to be made available to the session trace application.
ggsn: Specifies that the GGSN as network element and its associated interfaces is to be made available to the session trace application.
mme: Specifies that the MME as network element and its associated interfaces is to be made available to the session trace application.
pgw: Specifies that the P-GW as network element and its associated interfaces is to be made available to the session trace application.
sgw: Specifies that the S-GW as network element and its associated interfaces is to be made available to the session trace application.

---

collection-timer *sec*

Specifies the amount of time (in seconds) to wait from initial activation/data collection before data is reported to the Trace Collection Entity (TCE). *sec* must be an integer from 0 through 255.

---

tce-mode none

Specifies that session trace files are to be stored locally and must be pulled by the TCE.

---

tce-mode push transport sftp path *string* **username** *name* **{ encrypted password** *enc_pw* **| password** *password* **}**

Specifies that session trace files are to be pushed to the Trace Collection Entity (TCE).
sftp: Specifies that Secure FTP is used to push session trace files to the TCE.
path *string*: Specifies the directory path on the TCE where files will be placed.
username *name*: Specifies the username to be used when pushing files to the TCE.

encrypted password *enc_pw*: Specifies the encrypted password to be used when pushing files to the TCE.
password *password*: Specifies the password to be used when pushing files to the TCE.

Usage

Use this command to configure the file transfer methods and modes for subscriber session trace functionality and to how and where session trace files are sent after collection.
This configuration contains collection timer, UMTS/EPC network element, type of file transfer, and user credentials setting to send the collected trace files to the TCE.

Example

The following command configures the collection time for session traces to *30* seconds, identifies the network element as all elements (GGSN, MME, S-GW, and P-GW), and pushes session trace files to a TCE via SFTP into a directory named */trace/agw* using a username *admin* and a password of *pw123*:

```
session trace network-element all collection-timer 30 tce-mode push
transport sftp path /trace/agw username admin password pw123
```

The following command configures the collection time for session traces to *30* seconds, identifies the network element as an MME, and pushes session trace files to a TCE via SFTP into a directory named */trace/sgw* using a username *admin* and a password of *pw123*:

```
session trace network-element mme collection-timer 30 tce-mode push
transport sftp path /trace/mme username admin password pw123
```

The following command configures the collection time for session traces to *30* seconds, identifies the network element as GGSN, and pushes session trace files to a TCE via SFTP into a directory named */trace/ggsn* using a username *admin* and a password of *pw123*:

```
session trace network-element ggsn collection-timer 30 tce-mode push
transport sftp path /trace/ggsn username admin password pw123
```

sgsn-global

This command gives access to the SGSN Global configuration mode to set parameters relevant to the SGSN and HNB-GW as a whole.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

```
sgsn-global
```

Usage

Using this command moves into SGSN Global Configuration mode. In this mode, you can set system-wide parameters on SGSN and HNB-GW to perform the following tasks:
On SGSN:

- monitoring and managing TLLIs in the BSSGP layer.
- defining IMSI ranges used as filters in the operator policy selection process.

On HNB-GW:

- setting system-wide IPC message aggregation parameters

Example

Enter the SGSN Global configuration mode with the following:

```
sgsn-global
```

snmp authentication-failure-trap

Enables or disables the SNMP traps for authentication failures.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] snmp authentication-failure-trap
```

no

Disables SNMP traps for authentication failures. When omitted, SNMP traps for authentication failures will be generated.

Usage

Disables authentication failure traps if they are not of interest. At this time the option may be changed to support trouble shooting.
By default SNMP authentication failure traps are disabled.

snmp community

Configures the SNMP v1 and v2 community strings.

Product

All

Privilege

Security Administrator, Administrator

Syntax

snmp community *string* **[context** *ctx_name* **] [view** *view_name* **] [read-only | read-write]**

no snmp community *string*

no

The specified community string is removed from the configuration.

string

Specifies a community string whose options are to be modified. *string* must be an alphanumeric string of 1 through 31 characters.

context *ctx_name*

Default: community string applies to all contexts.
Specifies a the context to which the community string shall be applied. *ctx_name* must be an alphanumeric string of 1 through 1023 characters.

view *view_name*

Default: community string applies to all views.
Specifies the view to which the community string shall be applied. *view_name* must be an alphanumeric string of 1 through 1023 characters.

read-only | read-write

Default: read-only
Specifies if access rights for the community string.
read-only: the configuration may only be viewed.
read-write: the configuration may be viewed and edited.

Usage

The community strings define the privileges of SNMP users. It may be desirable to give read-only access to front line operators.

Example

snmp community *sampleString*

snmp community *sampleString* **context** *sampleContext*

snmp community *sampleString* **context** *sampleContext* **view** *sampleView*

snmp community *sampleString* **view** *sampleView* **read-write**

no snmp community *sampleString*

snmp engine-id

Configures the SNMP engine to use for SNMP requests when SNMPv3 agents are utilized.

Product

All

Privilege

Security Administrator, Administrator

Syntax

snmp engine-id local *id*

id

Specifies the SNMPv3 engine to employ. *id* must be an alphanumeric string of 1 through 31 characters.

Usage

When SNMPv3 is used for SNMP access to the chassis the engine ID can be used to quickly change which schema is used for SNMP access.

Important: The system can send either SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices. However, the Web Element Manager can only process SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) traps. If the SNMP target being configured is Web Element Manager application, then you must not configure this command to use.

Example

snmp engine-id local *id*

snmp heartbeat

Enables the sending of periodic “heartbeat” notifications (traps).

Product

All

Privilege

Administrator

Syntax

snmp heartbeat { interval [*minutes*] | second-interval [*seconds*] }

[deafult | no] snmp heartbeat

default

Returns the command to its default setting of disabled.

no

Disables the feature.

interval [*minutes*]

Default: 60
Specifies the interval time (in minutes) between notifications. *minutes* must be an integer from 1 through 1440.

second-interval [*seconds*]

Default: 30
Specifies the secondary interval time, in seconds, between notifications. *seconds* must be an integer from 10 through 50.

Usage

Use this command to enable the sending of a heartbeat notification periodically to confirm a system is up and communicating.

Example

The following command sets the SNMP heartbeat notification interval to 2 hours, 15 minutes and 30 seconds:

```
snmp heartbeat interval 135 second-interval 30
```

snmp history heartbeat

Enables the recording of heartbeat notifications in SNMP history.

Product

All

Privilege

Administrator

Syntax

```
[ default | no ] snmp history heartbeat
```

default

Returns the command to the default setting of enabled.

no

Disables the history recording feature.

Usage

Use this command to enable the recording of SNMP heartbeat notifications in SNMP history files.

snmp notif-threshold

Configures the number of SNMP notification that need to be generated for a given event before it is propagated to the SNMP users.

Product

All

Privilege

Security Administrator, Administrator

Syntax

snmp notif-threshold *count* **[low** *low_count* **] [period** *seconds* **]**

no snmp notif-threshold

no

Removes all SNMP notification thresholds. All notifications will be broadcast to SNMP users.

count

Default: 100
Specifies the number of notifications that must be generated before the next notification is broadcast to SNMP users. *count* must be an integer from 1 through 10000.

low *low_count*

Default: 20
Specifies the number of notifications within the monitoring period before which any subsequent notification for each specific event. *low_count* must be an integer from 1 through 10000.

period *seconds*

Default: 300
Specifies the number of seconds of the monitoring window size before any subsequent notification may be broadcast to users. *seconds* must be an integer from 10 through 3600.

Usage

Set the notification threshold to avoid a flood of events which may be the result of a single failure or maintenance activity.

Example

```
snmp notif-threshold 100

snmp notif-threshold 100 period 30
```

snmp server

Enables the SNMP server as well the configuration of the SNMP server port.

Product

All

Privilege

Security Administrator, Administrator

Syntax

snmp server [port *number* **]**

no snmp server

no

Restores the default SNMP port assignment.

port *number*

Default: 161
Specifies the port number to use for SNMP communications. *number* must be an integer from 1 to 65535.

Usage

Set the SNMP port for communications when SNMP is enabled.

Important: This will result in restarting the SNMP agent when the **no** keyword is omitted. SNMP queries as well as notifications/traps will be blocked until the agent has restarted.

Example

```
snmp server port 100

no snmp server
```

snmp target

Configures remote receivers for SNMP notifications.

Product

All

Privilege

Security Administrator, Administrator

Syntax

snmp target *name ip_address* **[port** *number* **] [non-default] [security-name** *string* **] [version { 1 | 2c | 3 | view] [security-level { noauth | { auth | priv-auth privacy [encrypted] des** *privpassword* **} authentication [encrypted] { md5 | sha }** *authpassword* **} } [informs | traps]**

no snmp target *name*

---

no

Removes the specified target as a receiver of unsolicited SNMP messages (traps).

---

authentication { md5 | sha } *authpassword*

Reads the authentication type and password if the security level of the SNMP messages is set to **auth** or **priv-auth**. Authentication types are:

- **md5**: Configures the hash-algorithm to implement MD5 per RFC 1321.
- **sha**: Specifies that the hash protocol is Secure Hash Algorithm.

---

security-level **{ noauth | { auth | priv-auth privacy [encrypted] des** *privpassword* **}**

Sets the security level of the SNMPv3 messages, as follows:

- **noauth**: No authentication and encryption is used.
- **auth**: Only authentication will be used.
- **priv-auth**: Both authentication and encryption will be used.
- **privacy des** *privpassword*: Reads the privacy type and password.

---

name

Specifies a logical name to use to refer to the remote receiver. *name* must be an alphanumeric string of 1 through 31 characters.

---

ip_address

Specifies the IP address of the receiver. *ip_address* must be specified using IPv4 dotted-decimal notation.

---

non-default

Specifies that this destination is only used for SNMP traps which have been specifically identified.

port *number*

Default: 162
Specifies the port which is to be used in communicating with the remote receivers. *number* must be an integer from 0 through 65535.

security-name *string*

Default: no community string included
Specifies the community string to use in the unsolicited messages. *string* must be an alphanumeric string of 1 through 31 characters.

version { 1 | 2c | 3 } | view

Default: 1
Specifies the SNMP version the target supports and consequently the version of the SNMP protocol to use for communications.

Important: The system can send either SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices.However, the Web Element Manager can only process SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) traps. If the SNMP target being configured is Web Element Manager application, then you must configure this command to use version 1 or version 2c.

informs | traps

Default: traps
Specifies the type of SNMP event to use to send notifications to SNPM targets. **traps** are unacknowledged (fire and forget) whereas **informs** require a response from the SNMP target.
If the notification type is set to **informs**, the notification is resent if no response is received within 5 seconds. The notification is resent at most two times.

Usage

The target manages the list of remote receivers to which unsolicited messages are sent. Use this command to add /remove a monitoring system to/from a network.

Example

```
snmp target sampleReceiver 1.2.3.4 security-name sampleComm

snmp target sampleReceiver 1.2.5.6 port 100

snmp target sampleReceiver 1.2.7.8 version 2c traps

no snmp target sampleReceiver
```

snmp trap

This command enables or disables generation of specific or all SNMP traps.

Product

All

Privilege

Security Administrator, Administrator

Syntax

snmp trap { enable | suppress } [*trap_name1 trap_name2 ... trap_nameN* **| all]**

enable

Enables or allows the generation of one or more SNMP traps by the system.

suppress

Disables the generation of one or more SNMP traps by the system.

trap_name1 trap_name2 ... trap_nameN

The name of the specific SNMP trap to enable or disable. Multiple traps can be listed for a single instance of this command.

Important: The system disregards character case (case insensitive) when entering trap names.

all

Default: Enable All
Specifies that all SNMP traps will be affected by the specified operation (enable or suppress).

Usage

SNMP traps are used by the system to indicate that certain events have occurred. A complete listing of the traps supported by the system and their descriptions can be found in the *SNMP MIB Reference*. Additionally, a trap listing can be viewed using the following command:

snmp trap { enable | suppress } ?

By default, the system enables the generation of all traps. However, individual traps can be disabled allowing only traps of a certain type or alarm level to be generated. This command can be used to disable un-desired traps and/or re-enable previously suppressed traps.

Example

The following command suppresses the LogMessage trap:

```
snmp trap suppress logmessage
```

The following command suppresses the *CLISessEnd* and *CLISessStart*:

```
snmp trap suppress clisessend clisessstart
```

snmp trap-timestamps

Adds an additional system-time varbind to generated traps.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] snmp trap-timestamps
```

no

Disables the adding of timestamps to generated traps.

Usage

The timestamp added to the generated trap reflects the current system time. The timestamp is proprietary. This functionality is disabled by default.

Important: If the Web Element Manager application is used as your alarm server, the application relies on the timestamp provided by enabling this command to identify duplicate traps. As a result, it is recommended that this parameter be enabled for this case.

Example

The following command enables the inclusion of a timestamp with each generated trap:

```
snmp trap-timestamps
```

snmp user

Configures an SNMPv3 user for SNMP access.

Product

All

Privilege

Security Administrator, Administrator

Syntax

snmp user *user_name* **[[encrypted] password** *password* **| engine** *id* **| group** *grp_name* **| security-model** *model* **auth [[encrypted] password** *password* **]]**

no snmp user *user_name*

---

no

Removes the specified user from the list of valid SNMPv3 users.

---

user_name

Specifies the user which is to use SNMPv3 interfaces to the system. *user_name* must be an alphanumeric string of 1 through 31 characters.

---

engine *id*

The SNMP engine ID. **id** must be an alphanumeric string of 1 through 31characters.

---

group *grp_name*

Default: undefined (not a member of any group)
Specifies the user SNMPv3 group the into which user will be added. *grp_name* must be an alphanumeric string of 1 to 1023 characters.

---

security-model *model* **auth**

Default: USM
Specifies the security model used to authenticate the user. *model* must be configured to the following:

- **usm**: User Security Model

[encrypted] password *password*

Default: undefined
Specifies the password for authenticating the user when the security model is set to User-based Security Model (USM).
The **encrypted** keyword indicates the password will be received in an encrypted form. *password* must be an alphanumeric string of 8 through 31 characters.
The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

Usage

Add and remove SNMPv3 users as operations staff or automated systems are updated. The security model will be user dependant based upon the support the users system provides.

Important: The system can send either SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices. However, the Web Element Manager can only process SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) traps. If the SNMP target being configured is Web Element Manager application, then you must not configure this command to use.

Example

```
snmp user user1

snmp user user1 security-model 2c auth

snmp user user1 group user1 group sampleGroup security-model usm auth

no snmp user user1
```

ss7-routing-domain

This command creates an SS7 routing domain instance and enters the SS7 Routing Domain Configuration mode.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

ss7-routing-domain *rd_id* **variant** *v_type* **[-noconfirm]**

no ss7-routing-domain *rd_id*

no

Removes the specified SS7 routing domain from the system configuration.

rd_id

Identifies a specific SS7 routing domain. Once it has been created, it can be accessed for further configuration and modification by entering the *rd_id* without entering the variant.
rd_id must be an integer from 1 through 12.

variant *v_type*

Identifies the national standard to be used for call setup, routing and control, signaling. Select one of the following:

- **ansi:** American National Standards Institute (U.S.A.)
- **bici:** Broadband Intercarrier Interface standard
- **china:** Chinese standard
- **itu:** International Telecommunication Union (ITU-T) Telecommunication Standardization Sector
- **ntt:** Japanese standard
- **ttc:** Japanese standard

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create an SS7 routing domain configuration instance or to enter the SS7 routing domain configuration mode to edit the configuration.
A routing domain groups configuration items to facilitate the management of the SS7 connection resources for an SGSN service. An Access Gateway supports up to 12 configured SS7 routing domains at one time.
After entering this command, the prompt appears as:
`[context_name]<hostname>(config-ss7-routing-domain-routing_domain_id)#`
For details about the commands and parameters used to define or edit an SS7 routing domain, refer *SS7 Routing Domain Configuration Mode* chapter.

Example

The following creates an SS7 routing domain with an index of *1* and the variant selection of Broadcast Intercarrier Interface (*bici*):

```
ss7-routing-domain 1 variant bici
```

The following command creates an SS7 routing domain instance with an index of *2* and the variant selection of Broadcast Intercarrier Interface (*bici*) to be associated with HNB RN-PLMN in an HNB access network:

```
ss7-routing-domain 1 variant bici
```

suspend local-user

Suspends a local-user administrative account.

Product

All

Privilege

Administrator

Syntax

[no] suspend local-user *name*

no

Removes the suspended status for the specified local-user account.

name

The name of the local-user account expressed as an alphanumeric string of 3 through 16 characters that is case sensitive.

Usage

This command allows a security administrator to suspend local-user administrative accounts.
A "suspended" user cannot login to the system. The user's account information (passwords, password history, etc.), however, is preserved.

Example

The following command suspends a local-user account called *Inspector1*:

```
suspend local-user Inspector1
```

The following command removes the suspension from a local-user account called *Admin300*:

```
no suspend local-user Admin300
```

system

Configures system information which is accessible via SNMP.

Product

All

Privilege

Security Administrator, Administrator

Syntax

system { carrier-id mcc *mcc_id* **mnc** *mnc_id* **| contact** *who* **| description** *string* **| hostname** *host_name* **| location** *text*| **sysdesc-sysoid-style [default | new] }**

default system { contact | location }

default

Removes the configured **system contact** and **system location** form the system.

carrier-id mcc *mcc_id* **mnc** *mnc_id*

Important: This carrier ID is not used by the GGSN

Specifies a carrier-id that is a unique identifier for the carrier that has installed the system. When the carrier ID values are set, the carrier-id and gmt_offset attributes are included in access-request and accounting packets when using the following RADIUS dictionaries:

- 3gpp2
- 3gpp2-835
- starent
- starent-835
- starent-vsa1
- starent-vsa1-835
- custom9

mcc *mcc_id*: The mobile country code. This must be specified as a 3-digit string from 001 through 999.
mnc *mnc_id*: The mobile network code. This must be specified as a 2- or 3-digit string from 01 through 999.

contact *who*

Default: No contact specified.
contact *who*: specifies the contact information for the chassis. *who* must be an alphanumeric string of 0 through 255 characters. The string must be embedded in double quotes (“) if spaces and special punctuation is to be used.

description *string*

Allows a user to describe the system for identification purposes. The system description can be comprised of a mix of alphanumeric characters, as follows:

- **%version%** - software version.

- **%build%** - software build number
- **%chassis%** - chassis type (ASR 5000)
- **%staros%** - OS type
- **%hostname%** - system name
- **%release%** - release number
- **%kerver%** - kernel version
- **%machine%** - machine hardware name
- *string* - an alphanumeric string of 1 through 255 characters.

hostname *host_name*

hostname *host_name*: configures the chassis host name where *host_name* must be an alphanumeric string of 1 through 63 characters.

Important: Please note that changing the chassis host name results in the command prompt changing as well to reflect the new name. This may affect any previously scripted interfaces from an OSS or maintenance facility.

location *text*

Default: No location specified.
location *text*: specifies the system location expressed as an alphanumeric string of 0 through 255 characters. The text specified must be embedded in double quotes (“) if spaces are to be used.

sysdesc-sysoid-style [default | new]

Allows the user to select the SNMP return for the objects sysDescr and sysOId.

- **default** - SNMP returns old style system description and old style system OID string.
- **new** - SNMP returns Cisco style system description and Cisco style OID string.

Usage

Specify system basic information which is useful back at a network operations center which uses the SNMP interfaces for management.

Example

The following commands configure the contact information, system host name, and location text, or remove configured location and system respectively.

```
system contact user1@company.com

system hostname system16

system location “Clark Street Closet\nBasement Rack 4”
```

The following commands remove the configured contact and location from system respectively

```
default system contact

default system location
```

tacacs mode

Enters the TACACS+ (Terminal Access Controller Access Control System+) configuration mode. Use this mode to configure up to three TACACS+ servers for use in authenticating administrative users via the TACACS+ protocol.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
tacacs mode
```

Usage

Enter TACACS Configuration Mode to configure up to three TACACS+ servers for use in authenticating administrative users via the TACACS+ protocol. For additional information, see the *TACACS+ Configuration Mode Commands* chapter.

Example

Use the following command to enter TACACS mode:

```
tacacs mode
```

task facility ipsecmgr

Configures IPSec manager settings.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
task facility ipsecmgr { ikev1 { task-count { increased | normal } } | task-count {
increased | normal } }
```

ikev1 { task-count { increased | normal } }

Default: **normal**
Adjusts the IPSec manager task count to support EHA for IKEv1. See **task-count** below.

task-count { increased | normal }

Default: **normal**
Adjusts the IPSec manager task count to support EHA.
increased: Starts additional IPSec manager tasks operating on the packet processing cards. In increased mode, they run on all but demux packet processing cards. Also, all the IPSec managers start at the same time when an active non-demux card is detected and IPSec is configured.
normal: Uses the standard algorithm for allocating memory for IPSec manager tasks. In normal mode, IPSec managers do not run on session packet processing cards.

Caution: If **task-count** is set to **normal** and session recovery is enabled, IPSec manager tasks are not allowed to start on most packet processing cards. Because the resources are not reserved, IPSec managers in normal mode only run on demux packet processing cards.

Usage

Sets IPSec manager parameters for all IPSec managers in the system.

Example

Use the following command to set the IPSec manager task count to **increased** mode:

```
task facility ipsecmgr task-count increased
```

task facility sessmgr

Configures system information which is accessible via SNMP.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
task { facility sessmgr start { aggressive | normal } | resource cpu-memory-low { kill |
warn } }
```

facility sessmgr start { aggressive | normal }

Default: Normal
Specifies the facility options for the session manager.
aggressive: specifies the maximum number of session manager processes are started immediately.

Caution: The **task facility sessmgr start aggressive** command should only be used if the system will reach capacity (for the existing configuration) during the first few minutes of service.

Caution: This command must only be executed last during configuration (or appended to the end of the configuration file) to ensure the availability of memory resources to contexts and services.

normal: indicates the session manager processes are started as needed.

resource cpu-memory-low { kill | warn }

Default: kill
Sets the action for the Resource Manager to take when the amount of free memory on a CPU falls below 12MB. An SNMP TRAP and CORBA notification are generated and the event is logged.
Once the free memory threshold is crossed, The Resource Manager examines all tasks on that cpu and finds the most over limit task and kills it. If there are no over limit tasks nothing happens. Resource Manager takes preference on killing a non-sessmgr task over a sessmgr task.
kill: The task most over memory limit (if any) is killed and recovered.
warn: The event is logged and no tasks are killed.

Usage

Set the session manager start policy to aggressive on heavily utilized systems to avoid undue delays in processing subscriber sessions.
Set the CPU memory low action to only log CPU low memory events.

Example

```
task facility sessmgr start aggressive

task facility sessmgr start normal

task resource cpu-memory-low warn
```

task facility acsmgr

This command configures ACSMgr task settings.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

```
task facility acsmgr start [ aggressive | normal ]

no task facility acsmgr start
```

no

Disables the configured ACSMgr setting.

aggressive

Specifies to start the maximum possible ACSMgr tasks.

normal

Configures the resource subsystem to start/stop ACSMgr tasks on an as-needed basis.

Usage

This command provides option for the resource subsystem to start maximum possible ACSMgr tasks based on the license configured and the available system configuration.

Example

The following command starts the maximum possible ACSMgr tasks:

```
task facility acsmgr start aggressive
```

terminal

Configures the console port on the SPIO.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
terminal [ carrierdetect { off | on } | databits { 7 | 8 } | flowcontrol { hardware { off
| on } | none } | parity { even | none | odd } | speed { 115200 | 19200 | 38400 | 57600 |
9600 } | stopbits { 1 | 2 } ]
```

carrierdetect { off | on }

Specifies whether or not the console port is to use Data Carrier Detect (DCD) when connecting to a terminal.
Default: off
off: Do not use DCD.
on: Use DCD.

databits { 7 | 8 }

Specifies the number of data bits used to transmit and receive characters.
Default: **8**
7: Use 7 databits to transmit and receive characters.
8: Use 8 databits to transmit and receive characters.

flowcontrol { hardware {off | on } | none }

Specifies how the flow of data is controlled between the SPIO and a terminal.
Default: **none**
hardware: Enables or disables the use of hardware-based flow control
off: Disables the use of Ready to Send (RTS) and Clear to Send (CTS).
on: Enables the use of Ready to Send (RTS) and Clear to Send (CTS).
none: Disables the use of DCD, RTS and CTS.

parity { even | none | odd }

Specifies the type of error checking used on the port.
Default: none
even - Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits even.
none - Disables error checking.
odd - Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits odd.

speed { 115200 | 19200 | 38400 | 57600 | 9600 }

Specifies the flow of data in bits per second between the console port and terminal.
Default: **9600**

stopbits { 1 | 2 }

Specifies the number of stop bits between each transmitted character.
Default: **1**
1: Use one stop bit between each transmitted character.
2: Use two stop bits between each transmitted character.

Usage

Sets the SPIO's console port parameters for communication with the terminal device.

Example

The following command sets the SPIO's console port. The terminal must support these values.

```
terminal carrierdetect off databits 7 flowcontrol hardware on parity even
speed 115200 stopbits 1
```

threshold 10sec-cpu-utilization

Configures a threshold that measures a 10-second average of cpu utilization. Its polling interval can be set down to 30 seconds.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold 10sec-cpu-utilization *percent* **[clear** *percent* **]**

percent

Default: 0
Configures Specifies the high threshold for 10-second average cpu-utilization. If the monitored CPU utilization is greater than or equal to the specified percentage an alert is sent. Regardless of the length of the polling interval, only one sample at the end of the polling interval is tested.

clear *percent*

Default: 0:
This is a low watermark value that sets the alarm clearing threshold value. If not specified it is taken from the first value.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set a threshold that sends an alert when CPU utilization over a 10-second average exceeds the limit set.
Alerts or alarms are triggered for 10-second sample of CPU utilization based on the following rules:

- **Enter condition:** 10-second average percentage of CPU utilization is greater than or equal to the high threshold.
- **Clear condition:** 10-second average percentage of CPU utilization is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Important: This command is not supported on all platforms.

Example

The following command generates an alert when the 10-second average CPU utilization reaches *45* percent:

```
threshold 10sec-cpu-utilization 45
```

threshold aaa-acct-archive-queue-size

This command configures AAA accounting archive thresholds based on the maximum values of session manager and ACS manager archive queue size.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
threshold aaa-acct-archive-queue-size1 percent [ clear percent ]

default threshold aaa-acct-archive-queue-size1 percent [ clear percent ]

threshold aaa-acct-archive-queue-size2 percent [ clear percent ]

default threshold aaa-acct-archive-queue-size2 percent [ clear percent ]

threshold aaa-acct-archive-queue-size3 percent [ clear percent ]

default threshold aaa-acct-archive-queue-size3 percent [ clear percent ]
```

percent

Configures Specifies the high threshold for monitoring the accounting message archive queue length. If the queue length is greater than or equal to the specified percentage an alarm is sent.
Default value for **aaa-acct-archive-queue-size1**: 25%
Default value for **aaa-acct-archive-queue-size2**: 50%
Default value for **aaa-acct-archive-queue-size3**: 90%

clear *percent*

This is a low watermark value that sets the alarm clearing threshold value. If not specified it is taken from the first value.
Default value for **aaa-acct-archive-queue-size1**: 25%
Default value for **aaa-acct-archive-queue-size2**: 50%
Default value for **aaa-acct-archive-queue-size3**: 90%

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

In the event that the system cannot communicate with configured AAA accounting servers (RADIUS or CGFs), either due to the server being busy or loss of network connectivity, the system buffers, or archives, the accounting messages.
Accounting message archive queue size thresholds generate alerts or alarms based on the queue length of AAA accounting messages buffered in the archive during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for accounting message archive queue size thresholds based on the following rules:

- **Enter condition:** Actual number of archived messages is greater than or equal to the high threshold.
- **Clear condition:** Actual number of archived messages less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command generates an alarm when *70*% of the AAA accounting message archive buffer is filled, and clears the alarm when the buffer size is reduced to *30*%:

```
threshold aaa-acct-archive-queue-size1 70 clear 30
```

threshold aaa-acct-archive-size

This command configures the accounting message archive size threshold.

Product

PDSN, GGSN, HA, ASN GW

Privilege

Security Administrator, Administrator

Syntax

threshold aaa-acct-archive-size *high_thresh* **[clear** *low_thresh* **]**

default threshold aaa-acct-archive-size

high_thresh

Default: 1
Specifies the high threshold number of archived accounting messages that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 1044000.

clear *low_thresh*

Default: 1
Specifies the low threshold number of archived accounting messages that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thresh* is an integer from 0 through 1044000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

In the event that the system cannot communicate with configured AAA accounting servers (RADIUS or CGFs), either due to the server being busy or loss of network connectivity, the system buffers, or archives, the accounting messages.
Accounting message archive size thresholds generate alerts or alarms based on the number of AAA accounting messages buffered in the archive during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.
Alerts or alarms are triggered for accounting failures based on the following rules:

- **Enter condition:** Actual number of archived messages that is greater than or equal to the high threshold.
- **Clear condition:** Actual number of archived messages that is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *250* AAA accounting archived messages and low threshold of *100* for a system using the Alarm thresholding model:

```
threshold aaa-acct-archive-size 250 clear 100
```

threshold aaa-acct-failure

Configures accounting failure thresholds for the system.

Product

PDSN, GGSN, HA, ASN GW

Privilege

Security Administrator, Administrator

Syntax

threshold aaa-acct-failure *high_thresh* **[clear** *low_thresh* **]**

default threshold aaa-acct-failure

high_thresh

Default: 0
Specifies the high threshold number of accounting failures that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of accounting failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Accounting failure thresholds generate alerts or alarms based on the number of failed AAA accounting message requests that occur during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.
Alerts or alarms are triggered for accounting failures based on the following rules:

- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *100* AAA accounting failures and low threshold of *25* for a system using the Alarm thresholding model:

```
threshold aaa-acct-failure 100 clear 25
```

threshold aaa-acct-failure-rate

Configures accounting failure rate thresholds for the system.

Product

PDSN, GGSN, HA, ASN GW

Privilege

Security Administrator, Administrator

Syntax

threshold aaa-acct-failure-rate *high_thresh* **[clear** *low_thresh* **]**

default threshold aaa-acct-failure-rate

high_thresh

Default: 1
Specifies the high threshold percent of accounting failures that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 and 100.

clear *low_thresh*

Default: 1
Specifies the low threshold percent of accounting failures that maintains a previously generated alarm condition. If the percentage of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thresh* is an integer from 0 through 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Accounting failure rate thresholds generate alerts or alarms based on the percentage of AAA accounting message requests that failed during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.
Alerts or alarms are triggered for accounting failure rates based on the following rules:

- **Enter condition:** Actual failure percentage is greater than or equal to the high threshold.
- **Clear condition:** Actual failure percentage is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a AAA accounting failure rate high threshold percentage of *30* and a low threshold percentage of *10* for a system using the Alarm thresholding model:

```
threshold aaa-acct-failure-rate 30 clear 10
```

threshold aaa-auth-failure

Configures authentication failure thresholds for the system.

Product

PDSN, GGSN, HA, ASN GW

Privilege

Security Administrator, Administrator

Syntax

threshold aaa-auth-failure *high_thresh* **[clear** *low_thresh* **]**

default threshold aaa-auth-failure

high_thresh

Default: 0
Specifies the high threshold number of authentication failures that must be met or exceeded within the polling interval to generate an alert or alarm.*high_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of authentication failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Authentication failure thresholds generate alerts or alarms based on the number of failed AAA authentication message requests that occur during the specified polling interval. Authentication requests are counted for all AAA authentication servers that the system is configured to communicate with.
Alerts or alarms are triggered for authentication failures based on the following rules:

- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *100* AAA authentication failures for a system using the Alert thresholding model:

```
threshold aaa-auth-failure 100
```

threshold aaa-auth-failure-rate

Configures authentication failure rate thresholds for the system.

Product

PDSN, GGSN, HA, ASN GW

Privilege

Security Administrator, Administrator

Syntax

threshold aaa-auth-failure-rate *high_thresh* **[clear** *low_thresh* **]**

default threshold aaa-auth-failure-rate

high_thresh

Default: 5
Specifies the high threshold percent of authentication failures that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 100.

clear

Allows the configuration of Specifies the low threshold.

low_thresh

Default: 5
Specifies the low threshold percent of authentication failures that maintains a previously generated alarm condition. If the percentage of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thresh* is an integer from 0 through 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Authentication failure rate thresholds generate alerts or alarms based on the percentage of AAA authentication message requests that failed during the specified polling interval. Authentication requests are counted for all AAA authentication servers that the system is configured to communicate with.
Alerts or alarms are triggered for authentication failures based on the following rules:

- **Enter condition:** Actual failure percentage is greater than or equal to the high threshold.
- **Clear condition:** Actual failure percentage is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a AAA authentication failure rate high threshold percentage of *30* for a system using the Alert thresholding model:

```
threshold aaa-auth-failure-rate 30
```

threshold aaa-retry-rate

Configures AAA retry rate thresholds for the system.

Product

PDSN, GGSN, HA, ASN GW

Privilege

Security Administrator, Administrator

Syntax

threshold aaa-retry-rate *high_thresh* **[clear** *low_thresh* **]**

default threshold aaa-retry-rate

high_thresh

Default: 5
Specifies the high threshold percent of AAA request message retries that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 100.

clear *low_thresh*

Default: 5
Specifies the low threshold percent of AAA request message retries that maintains a previously generated alarm condition. If the percentage of retries falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thresh* is an integer from 0 through 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

AAA request message retry rate thresholds generate alerts or alarms based on the percentage of request messages (both authentication and accounting) that were retried during the specified polling interval. The percentage is based on a message count taken for all AAA authentication and accounting servers that the system is configured to communicate with.
Alerts or alarms are triggered for request message retries based on the following rules:

- **Enter condition:** Actual retry percentage is greater than or equal to the high threshold.
- **Clear condition:** Actual retry percentage is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a AAA message retry rate high threshold percentage of *25* and a low threshold percentage of *10* for a system using the Alarm thresholding model:

```
threshold aaa-retry-rate 25 clear 10
```

threshold aaamgr-request-queue

This command configures the AAA Manager internal request queue threshold.

Product

PDSN, GGSN, HA, ASN GW

Privilege

Security Administrator, Administrator

Syntax

threshold aaamgr-request-queue *high_thresh* **[clear** *low_thresh* **]**

default threshold aaamgr-request-queue

high_thresh

Default: 0
Specifies the high threshold number of AAA Manager Requests that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 1 through 100.

clear

Allows the configuration of Specifies the low threshold.

low_thresh

Default: 5
Specifies the low threshold number of AAA Manager Requests that maintains a previously generated alarm condition. If the percentage of failures falls beneath the low threshold within the polling interval, a clear alarm is generated. *low_thresh* is an integer from 0 through 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

AAA Manager Request thresholds generate alerts or alarms based on the number of AAA Manager Requests for an AAA manager process during the specified polling interval.
Alerts or alarms are triggered for AAA Manager Requests based on the following rules:

- **Enter condition:** Actual number of AAA Manager Requests per AAA manager is greater than or equal to the high threshold.
- **Clear condition:** Actual number of AAA Manager Requests per AAA manager process is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm is not generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a AAA authentication failure rate high threshold percentage of *30* for a system using the Alert thresholding model:

```
threshold aaamgr-request-queue 30
```

threshold asngw-auth-failure

Configures authentication failure thresholds for the ASN-GW system.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

threshold asngw-auth-failure *high_thresh* **[clear** *low_thresh* **]**

default threshold asngw-auth-failure

high_thresh

Default: 0
Specifies the high threshold number of authentication failures that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of authentication failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to configure threshold limits to generate alerts or alarms based on the number of failed ASN-GW authentication message requests that occur during the specified polling interval. Authentication requests are counted for all ASN Gateway authentication servers with which that the system is configured to communicate.
Alerts or alarms are triggered for authentication failures based on the following rules:

- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *100* authentication failures for an ASN-GW using the Alert thresholding model:

```
threshold asngw-auth-failure 100
```

threshold asngw-handoff-denial

Configures thresholds for hand-off denial for the ASN-GW service.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

threshold asngw-handoff-denial *high_thresh* **[clear** *low_thresh* **]**

default threshold asngw-handoff-denial

high_thresh

Default: 0
Specifies the high threshold number of hand-off denials that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of hand-off denials that maintains a previously generated alarm condition. If the number of hand-off denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set threshold limits to generate alerts or alarms based on the number of denied hand-off that occurred during the specified polling interval. Hand-off denial messages are counted for all ASN Gateways that the system is configured to communicate with.
Alerts or alarms are triggered for hand-off denials based on the following rules:

- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *100* hand-off denials using the Alert thresholding model:

```
threshold asngw-handoff-denial 100
```

threshold asngw-max-eap-retry

Configures thresholds for maximum retries for Extensible Authentication Protocol (EAP) authentication on an ASN-GW service.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

threshold asngw-max-eap-retry *high_thresh* **[clear** *low_thresh* **]**

default threshold asngw-max-eap-retry

high_thresh

Default: 0
Specifies the high threshold number of retries for EAP authentication that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of retries for EAP authentication that maintains a previously generated alarm condition. If the number of retries falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set threshold limits to generate alerts or alarms based on the number of retries for EAP authentication that occur during the specified polling interval.
Alerts or alarms are triggered for maximum number of retries for EAP authentication based on the following rules:

- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *100* alerts or alarms generated on maximum number of retries for EAP authentication for an ASN Gateway using the Alert thresholding model:

```
threshold asngw-handoff-denial 100
```

threshold asngw-network-entry-denial

Configures thresholds for denial of network entry to an MS with in the ASN-GW service.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

threshold asngw-network-entry-denial *high_thresh* **[clear** *low_thresh* **]**

default threshold asngw-network-entry-denial

high_thresh

Default: 0
Specifies the high threshold number of denial of network entry to an MS that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of denial of network entry to an MS that maintains a previously generated alarm condition. If the number of denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set threshold limits to generate alerts or alarms based on the number of network entry denials that occurred during the specified polling interval. Network denial messages are counted for an MS with which the system is configured to communicate.
Alerts or alarms are triggered for network entry denials based on the following rules:

- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *100* network entry denials for an MS using the Alert thresholding model:

```
threshold asngw-network-entry-denial 100
```

threshold asngw-r6-invalid-nai

Configures thresholds to generate alert/alarm for invalid Network Access Identifier (NAI) in R6 message.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

threshold asngw-r6-invalid-nai *high_thresh* **[clear** *low_thresh* **]**

default threshold asngw-r6-invalid-nai

high_thresh

Default: 0
Specifies the high threshold number of invalid NAIs in R6 messages that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of invalid NAIs in R6 messages that maintains a previously generated alarm condition. If the number of denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set threshold limits to generate alerts or alarms based on the number of invalid NAIs in R6 messages that occurred during the specified polling interval. Invalid NAIs are counted for an MS that the system is configured to communicate with or per system for all R6 messages.
Alerts or alarms are triggered for invalid NAIs based on the following rules:

- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *100* invalid NAIs in R6 messages using the Alert thresholding model:

```
threshold asngw-r6-invalid-nai 100
```

threshold asngw-session-setup-timeout

Configures thresholds to generate alert/alarm for session setup timeouts in an ASN-GW service.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

threshold asngw-session-setup-timeout *high_thresh* **[clear** *low_thresh* **]**

default threshold asngw-session-setup-timeout

high_thresh

Default: 0
Specifies the high threshold number of timeouts during session setup that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of timeouts during session setup that maintains a previously generated alarm condition. If the number of denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set threshold limits to generate alerts or alarms based on the number of timeouts during session setup that occurred during the specified polling interval.
Alerts or alarms are triggered for session setup timeouts based on the following rules:

- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *100* timeouts during session setup using the Alert thresholding model:

```
threshold asngw-session-setup-timeout 100
```

threshold asngw-session-timeout

Configures thresholds to generate alert/alarm for session timeouts in an ASN-GW service.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

threshold asngw-session-timeout *high_thresh* **[clear** *low_thresh* **]**

default threshold asngw-session-timeout

high_thresh

Default: 0
Specifies the high threshold number of timeouts during session that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of timeouts during session that maintains a previously generated alarm condition. If the number of session timeouts falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set threshold limits to generate alerts or alarms based on the number of timeouts during a session that occurred during the specified polling interval.
Alerts or alarms are triggered for session timeouts based on the following rules:

- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *100* timeouts during a session using the Alert thresholding model:

```
threshold asngw-session-timeout 100
```

threshold call-reject-no-resource

Configures thresholds on the system for calls rejected due to insufficient resources.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold call-reject-no-resource *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of no-resource call rejects issued by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
The number is an integer from 0 through 100000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of no-resource call rejects issued by the system that maintains a previously generated alarm condition. If the number of rejections falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number is an integer from 0 through 100000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

No resource call reject thresholds generate alerts or alarms based on the total number of calls that were rejected by the system due to insufficient or no resources (memory and/or session licenses) during the specified polling interval.
Alerts or alarms are triggered for no-resource-rejected calls based on the following rules:

- **Enter condition:** Actual number of calls rejected due to no resources is greater than or equal to the high threshold.
- **Clear condition:** Actual number of calls rejected due to no resources is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count for the number of calls rejected by the system due to insufficient or no resources to *100* and allow threshold of *40* for a system using the Alarm thresholding model:

```
threshold call-reject-no-resource 100 clear 40
```

threshold call-setup

Configures call setup thresholds for the system.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold call-setup *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of calls setup by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 100000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of calls setup by the system that maintains a previously generated alarm condition. If the number of setups falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 100000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Call setup thresholds generate alerts or alarms based on the total number of calls setup by the system during the specified polling interval.
Alerts or alarms are triggered for call setups based on the following rules:

- **Enter condition:** Actual number of call setups is greater than or equal to the high threshold.
- **Clear condition:** Actual number of call setups is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of 100 calls setup for a system using the Alert thresholding model:

```
threshold call-setup 100
```

threshold call-setup-failure

Configures call setup failure thresholds for the system.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold call-setup-failure *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of call setup failures experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 100000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of call setup failures experienced by the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 100000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Call setup failure thresholds generate alerts or alarms based on the total number of call setup failures experienced by the system during the specified polling interval.
Alerts or alarms are triggered for call setup failures based on the following rules:

- **Enter condition:** Actual number of call setup failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of call setup failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *100* call setup failures and a low threshold of *80* for a system using the Alarm thresholding model:

```
threshold call-setup-failure 100 clear 80
```

threshold cpu-available-memory

Configures thresholds for available CPU memory for the system.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
threshold cpu-available-memory low_thresh  [ clear high_thresh ]
```

low_thresh

Default: 32
Specifies the low threshold amount of CPU memory that must be met or exceeded at the polling time to generate an alert or alarm.
low_thresh is measured in megabytes (MB) and is an integer from 0 through 2048.

clear *high_thresh*

Default: 32
Specifies the high threshold amount of CPU memory that maintains a previously generated alarm condition. If the memory amount rises above the high threshold within the polling interval, a clear alarm will be generated.
high_thresh is measured in megabytes (MB) and is an integer from 0 through 2048.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

CPU available memory thresholds generate alerts or alarms based on the amount of available memory for each packet processing card CPU at the polling time. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU.
Alerts or alarms are triggered for available CPU memory based on the following rules:

- **Enter condition:** Average measured amount of memory/CPU for the last 5 minutes is less than or equal to the low threshold.
- **Clear condition:** Average measured amount of memory/CPU for the last 5 minutes is greater than the high threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Important: This command is not supported on all platforms.

Example

The following command configures a low threshold count of *50* MB CPU memory available and a high threshold of *112* MB for a system using the Alarm thresholding model:

```
threshold cpu-available-memory 50 clear 112
```

threshold cpu-load

Configures the threshold for monitoring packet processing card CPU loads using a 5-minute average measurement. The threshold is enabled by enabling CPU resource monitoring.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold cpu-load *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
If the monitored CPU load is greater than or equal to the specified number an alert is sent. *high_thresh* must be an integer from 0 through 15.

clear *low_thresh*

Default: 0
This is a low watermark value that sets the alarm clearing threshold value. If not present it is taken from the first value. *low_thresh* must be an integer from 0 through 15.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to Specifies the low threshold.

Usage

Use this command to set an alert when the card's CPU load is equal to or greater than the number specified. Alerts or alarms are triggered for CPU load based on the following rules:

- **Enter condition:** Actual CPU load is greater than or equal to the high threshold.
- **Clear condition:** Actual CPU load is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Important: This command is not supported on all platforms.

Example

To set an alert when the packet processing card CPU load is over *10* and set an alert clear when the CPU load drops down equal or less than *7*, enter the following command;

```
threshold cpu-load 10 clear 7
```

threshold cpu-memory-usage

Configures the threshold for monitoring the percentage of total CPU memory used during the polling interval.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold cpu-memory-usage *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold for percentage of total memory used that must be met or exceeded at the end of the polling interval to generate an alert or alarm.
high_thresh is measured as a percentage of total CPU memory used and is an integer from 0 and 100. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold for percentage of total CPU memory used that maintains a previously generated alarm condition. If the memory usage falls below the low threshold within the polling interval, a clear alarm is generated.
low_thresh is measured as a percentage of total CPU memory used and is an integer from 0 and 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to Specifies the low threshold.

Usage

CPU memory usage generate alerts or alarms based on the percentage of total CPU memory used during the polling interval.
Alerts or alarms are triggered for CPU memory usage session based on the following rules:

- **Enter condition:** Actual percentage of CPU memory usage is greater than or equal to the specified percentage of total CPU memory.
- **Clear condition:** Actual CPU memory usage is less than the specified clear percentage of total CPU memory usage.

If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a threshold of *65* percent of total packet processing card CPU memory usage and a clear threshold of *35* percent:

```
threshold cpu-memory-usage 65 clear 35
```

threshold cpu-orbs-crit

Configures threshold for generating critical-level alerts or alarms based on the percentage of CPU utilization by the Object Request Broker System (ORBS) software task

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold cpu-orbs-crit *high_thresh* **[clear** *low_thresh* **]**

[default] threshold cpu-orbs-crit

default

Restores this parameter to its default setting.

high_thresh

Default: 60
Specifies the high threshold percent of CPU utilization by the ORB software task that must be exceeded as measured at the time of polling to generate a critical-level alert or alarm.
high_thresh is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.

clear *low_thresh*

Default: 60
Specifies the low threshold percent of CPU utilization by the ORB software task that maintains a previously generated alarm condition. If the percentage is measured as less than or equal to Specifies the low threshold at the time of polling, a clear alarm will be generated.
low_thresh is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to Specifies the low threshold.

Usage

Object Request Broker (ORB) software task CPU utilization thresholds generate critical-level alerts or alarms based on the percentage of packet processing card CPU resources it is consuming at the time of polling. Critical-level alerts or alarms are triggered for CPU usage by the ORBs software task based on the following rules:

- **Enter condition:** Actual CPU usage percentage is greater than the high threshold.
- **Clear condition:** Actual CPU usage percentage is less than or equal to the low threshold.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a critical-level alarm threshold of *35* percent of CPU utilization by the ORBS task and a clear threshold of *35* percent:

```
threshold cpu-orbs-crit 35 clear 35
```

threshold cpu-orbs-warn

Configures threshold for generating warning-level alerts or alarms based on the percentage of CPU utilization by the Object Request Broker System (ORBS) software task

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold cpu-orbs-warn *high_thresh* **[clear** *low_thresh* **]**

[default] threshold cpu-orbs-warn

default

Restores this parameter to its default setting.

high_thresh

Default: 50
Specifies the high threshold percent of CPU utilization by the ORBS software task that must be exceeded as measured at the time of polling to generate a warning-level alert or alarm.
high_thresh is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.

clear *low_thresh*

Default: 50
Specifies the low threshold percent of CPU utilization by the ORBS software task that maintains a previously generated alarm condition. If the percentage is measured as less than or equal to Specifies the low threshold at the time of polling, a clear alarm will be generated.
low_thresh is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to Specifies the low threshold.

Usage

Object Request Broker (ORB) software task CPU utilization thresholds generate warning-level alerts or alarms based on the percentage of packet processing card CPU resources it is consuming at the time of polling.
Warning-level alerts or alarms are triggered for CPU usage by the ORBS software task based on the following rules:

- **Enter condition:** Actual CPU usage percentage is greater than the high threshold.
- **Clear condition:** Actual CPU usage percentage is less than or equal to the low threshold.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a warning-level alarm threshold of *25* percent of CPU utilization by the ORBS task and a clear threshold of *25* percent:

```
threshold cpu-orbs-warn 25 clear 25
```

threshold cpu-session-throughput

Configures thresholds for CPU session throughput for the system.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold cpu-session-throughput *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold session throughput that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is measured in kilobytes per second (Kbps) and is an integer from 0 through 1000000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold session thereabout that maintains a previously generated alarm condition. If the throughput falls below Specifies the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is measured in kilobytes per second (Kbps) and is an integer from 0 through 1000000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

CPU session throughput thresholds generate alerts or alarms based on total throughput for all Session Manager tasks running on each packet processing card CPU during the polling interval. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU.
Alerts or alarms are triggered for CPU session throughput based on the following rules:

- **Enter condition:** Actual CPU session throughput is greater than or equal to the high threshold.
- **Clear condition:** Actual CPU session throughput is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Important: This command is not supported on all platforms.

Example

The following command configures a high threshold count of *900* Kbps session throughput and a low threshold of *500* KBps for a system using the Alarm thresholding model:

```
threshold cpu-session-throughput 900 clear 500
```

threshold cdr-file-space

Configures the threshold for monitoring the percentage of total file space allocated for Charging Data Records (CDRs) used during the polling interval.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

threshold cdr-file-space *high_thresh* **[clear** *low_thresh* **]**

default threshold cdr-file-space

default

Configures this command with the default threshold settings.

high_thresh

Specifies the high threshold for percentage of total allocated CDR file space used that must be met or exceeded at the end of the polling interval to generate an alert or alarm.
high_thresh is measured in percentage of total allocated CDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.
Default: 90

clear *low_thresh*

Specifies the low threshold for percentage of total allocated CDR file space used that maintains a previously generated alarm condition. If the space usage falls below Specifies the low threshold within the polling interval, a clear alarm is generated.
low_thresh is measured in percentage of total allocated CDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.
Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to Specifies the low threshold.

Usage

CDR file space usage generate alerts or alarms based on the percentage of total allocated CDR file space used during the polling interval.
Alerts or alarms are triggered for CDR file space usage session based on the following rules:

- **Enter condition:** Actual percentage of allocated CDR file space usage is greater than or equal to the specified percentage of total CDR file space.
- **Clear condition:** Actual CDR file space used is less than the specified clear percentage of total allocated CDR file space usage.

If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a threshold of *65* percent of total allocated CDR file space usage and a clear threshold of *35* percent:

```
threshold cdr-file-space 65 clear 35
```

threshold contfilt-block

Configures the threshold for Content Filtering rating operations blocked during a polling interval at which the threshold are raised or cleared.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

threshold contfilt-block *high_thresh_value* **[clear** *low_thresh_value* **]**

default threshold contfilt-block

default

Configures this command with the default threshold settings.

high_thresh

Specifies the high threshold for number of rating operations blocked for content filtering service that must be met or exceeded at the end of the polling interval to generate an alert or alarm.
high_thresh is measured in numbers of total rating operations blocked and is an integer from 0 through 1000000. A value of 0 disables the threshold.

clear *low_thresh*

Specifies the low threshold for the total number of rating operations blocked for a content filtering service that maintains a previously generated alarm condition. If the threshold falls below Specifies the low threshold within the polling interval, a clear alarm is generated.
low_thresh is measured in numbers of total rating operations blocked and is an integer from 0 through 1000000. A value of 0 disables the threshold.
Default: 0

Usage

Use this command to configure the threshold for a content filtering service to generates alerts or alarms based on the number of rating operations blocked for a content filtering service during the polling interval.
If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll contfilt-block** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a threshold of *65000* rating operations blocked and a clear threshold of *35000* operations:

```
threshold contfilt-block 65000 clear 35000
```

threshold contfilt-rating

Configures the threshold for Content Filtering rating operations performed during a polling interval at which the threshold are raised or cleared.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

threshold contfilt-rating *high_thresh_value* **[clear** *low_thresh_value* **]**

default threshold contfilt-rating

default

Configures this command with the default threshold settings.

high_thresh

Specifies the high threshold for number of rating operations performed for content filtering service that must be met or exceeded at the end of the polling interval to generate an alert or alarm.
high_thresh is measured in numbers of total rating operations performed and is an integer from 0 through 1000000. A value of 0 disables the threshold.

clear *low_thresh*

Specifies the low threshold for the total number of rating operations performed for a content filtering service that maintains a previously generated alarm condition. If the threshold falls below Specifies the low threshold within the polling interval, a clear alarm is generated.
low_thresh is measured in umber of total rating operations performed and is an integer from 0 through 1000000. A value of 0 disables the threshold.
Default: 0

Usage

Use this command to configure the threshold for a content filtering service to generates alerts or alarms based on the number of rating operations performed for a content filtering service during the polling interval.
If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll contfilt-rating** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a threshold of *65000* percent of total rating operations performed and a clear threshold of *35000* percent:

```
threshold contfilt-rating 65000 clear 35000
```

threshold cpu-utilization

Configures thresholds for CPU utilization for the system.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold cpu-utilization *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 85
Specifies the high threshold CPU utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 100.

clear *low_thresh*

Default: 85
Specifies the low threshold CPU utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

CPU utilization thresholds generate alerts or alarms based on the utilization percentage of each packet processing card CPU during the specified polling interval. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU.
Alerts or alarms are triggered for CPU utilization based on the following rules:

- **Enter condition:** Average measured CPU utilization for the last 5 minutes
- **Clear condition:** Average measured CPU utilization for the last 5 minutes is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Important: This command is not supported on all platforms.

Example

The following command configures a high threshold CPU utilization percentage of *90* for a system using the Alert thresholding model:

```
threshold cpu-utilization 90
```

threshold dcca-bad-answers

Configures the threshold for invalid or bad responses to the system from Diameter server.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

threshold dcca-bad-answers *high_thresh* **[clear** *low_thresh* **]**

default threshold dcca-bad-answers

default

Disables the threshold for configured alarm and set the *high_thresh* and *low_thresh* values to 0.

high_thresh

Default: 0
Specifies the high threshold number of invalid messages or responses that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 1000000.

clear *low_thresh*

Default: 0
Specifies the low threshold number of invalid messages/responses that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 1000000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

In the event that the system receives invalid message or response from Diameter server **dcca-bad-answers** is generated.
DCCA bad answer messages size threshold generates alerts or alarms based on the number of invalid response or messages received during the specified polling interval.
Alerts or alarms are triggered for DCCA bad answers based on the following rules:

- **Enter condition:** Actual number of DCCA bad answer messages is greater than or equal to the high threshold.
- **Clear condition:** Actual number of DCCA bad answer messages is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Example

The following command configures a high threshold count of *250* DCCA bad answer messages and low threshold of *100* for a system using the Alarm thresholding model:

```
threshold dcca-bad-answers 250 clear 100
```

threshold dcca-protocol-error

Configures the threshold for Diameter Credit Control Application (DCCA) protocol error from Diameter server.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

threshold dcca-protocol-error *high_thresh* **[clear** *low_thresh* **]**

default threshold dcca-protocol-error

default

Disables the threshold for configured alarm and sets the *high_thresh* and *low_thresh* values to 0.

high_thresh

Default: 0
Specifies the high threshold number of protocol error received from Diameter server that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 1000000.

clear *low_thresh*

Default: 0
Specifies the low threshold number of protocol error received from Diameter server that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 1000000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

In the event that the system receives the protocol errors from Diameter server, **dcca-protocol-error** is generated.
DCCA protocol error threshold generates alerts or alarms based on the number of protocol error messages received from Diameter server during the specified polling interval.
Alerts or alarms are triggered for DCCA protocol error based on the following rules:

- **Enter condition:** Actual number of DCCA protocol error is greater than or equal to the high threshold.
- **Clear condition:** Actual number of DCCA protocol errors is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Example

The following command configures a high threshold count of *250* protocol errors and low threshold of *100* for a system using the Alarm thresholding model:

```
threshold dcca-protocol-error 250 clear 100
```

threshold dcca-rating-failed

Configures Diameter Credit Control Application (DCCA) Rating Group (content-id) request reject thresholds.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

threshold dcca-rating-failed *high_thresh* **[clear** *low_thresh* **]**

default threshold dcca-rating-failed

default

Disables the threshold for configured alarm and sets the *high_thresh* and *low_thresh* values to 0.

high_thresh

Default: 0
Specifies the high threshold number of requests for a block of credits due to invalid Rating Group (content-id), rejected from the Diameter server that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 1000000.

clear *low_thresh*

Default: 0
Specifies the low threshold number of requests for a block of credits due to invalid Rating Group (content-id), rejected from the Diameter server that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 1000000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

In the event that the Diameter server rejects the system request for a block of credits due to invalid Rating Group, defined as content-id, **dcca-rating-failed** message is generated.
Rating Group failed threshold generates alerts or alarms based on the number of requests rejected from Diameter server during the specified polling interval.
Alerts or alarms are triggered for Rating Group failed based on the following rules:

- **Enter condition:** Actual number of DCCA Rating Group failed is greater than or equal to the high threshold.
- **Clear condition:** Actual number of DCCA Rating Group failed is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Example

The following command configures a high threshold count of *250* requests rejected and low threshold of *100* for a system using the Alarm thresholding model:

```
threshold dcca-rating-failed 250 clear 100
```

threshold dcca-unknown-rating-group

Configures the unknown Diameter Credit Control Application (DCCA) Rating Group (content-id) returned by Diameter to system thresholds.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

threshold dcca-unknown-rating-group *high_thresh* **[clear** *low_thresh* **]**

default threshold dcca-unknown-rating-group

default

Disables the threshold for configured alarm and sets the *high_thresh* and *low_thresh* values to 0.

high_thresh

Default: 0
Specifies the high threshold number of unknown Rating Group (content-id) sent by the Diameter server and received by system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 1000000.

clear *low_thresh*

Default: 0
Specifies the low threshold number of unknown Rating Group (content-id) sent by Diameter server and received by system that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 1000000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

In the event that the Diameter server sends invalid Rating Groups, **content-ids** to the system, **dcca-unk-rating-group** message is generated.
Unknown Rating Group threshold generates alerts or alarms based on the number of unknown Rating Groups received by the system from Diameter server during the specified polling interval.
Alerts or alarms are triggered for unknown rating groups based on the following rules:

- **Enter condition:** Actual number of unknown rating groups is greater than or equal to the high threshold.
- **Clear condition:** Actual number of unknown rating groups is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Example

The following command configures a high threshold count of *250* unknown rating groups and low threshold of *100* for a system using the Alarm thresholding model:

```
threshold dcca-unknown-rating-group 250 clear 100
```

threshold diameter diameter-retry-rate

This command configures Diameter Retry Rate threshold for generating alerts or alarms based on the percentage of Diameter requests that were retried during the polling interval.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

threshold diameter diameter-retry-rate *high_thresh* **[clear** *low_thresh* **]**

default threshold diameter diameter-retry-rate

default

Configures this command with the default threshold settings.
Default: 0—disabled

high_thresh

Specifies the high threshold. If, within the polling interval, the percentage of Diameter requests retried equals or exceeds *high_thresh* an alert or alarm is generated.
high_thresh is an integer from 0 through 100.
Default: 0

clear *low_thresh*

Specifies the low threshold. If, within the polling interval, the percentage of Diameter requests retried falls below *low_thresh*, a clear alarm is generated.
low_thresh is an integer from 0 through 100.
Default: 0

Important: This value is applicable for the Alarm mode, and ignored for the Alert mode. In addition, if this value is not configured for the Alarm mode, the system assumes it is identical to the high threshold.

Usage

Diameter Retry Rate threshold generates alerts or alarms based on the percentage of Diameter requests that were retried during the specified polling interval.
Alerts or alarms are triggered based on the following rules:

- **Enter condition:** Percentage of Diameter requests retried is greater than or equal to the high threshold.
- **Clear condition:** Percentage of Diameter requests retried is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Example

The following command configures a high threshold of *75* percent, and a low threshold of *50* percent for a system using the Alarm thresholding model:

```
threshold diameter diameter-retry-rate 75 clear 50
```

threshold dns-learnt-ip-max-entries

This command configures thresholds for the percentage of total DNS-learnt IP entries in relation to the ACS DNS Snooping feature.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

threshold dns-learnt-ip-max-entries *high_thresh* **[clear** *low_thresh* **]**

default threshold dns-learnt-ip-max-entries

default

Configures this command with the default threshold setting.
Default: 90 percent. It is the same for both high and low thresholds.

high_thresh

Default: 90 percent
Specifies the high threshold for percentage of total DNS-learnt IP entries. When the percentage of total DNS-learnt IP entries meets or exceeds the high threshold at the end of the polling interval, an alert or alarm is generated.
When the percentage of total DNS-learnt IPv4 entries meets or exceeds the high threshold, the ECSTotalDNSLearntIPv4Threshold trap is generated.
When the percentage of total DNS-learnt IPv6 entries meets or exceeds the high threshold, the ECSTotalDNSLearntIPv6Threshold trap is generated.
high_thresh is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

clear *low_thresh*

Default: 90 percent
Specifies the low threshold for percentage of total DNS-learnt IP entries. When the percentage of total DNS-learnt IP entries goes below the low threshold within the polling interval, a clear alarm is generated.
When the percentage of total DNS-learnt IPv4 entries goes below the low threshold, the ECSTotalDNSLearntIPv4ThresholdClear trap is generated.
When the percentage of total DNS-learnt IPv6 entries goes below the low threshold, the ECSTotalDNSLearntIPv6ThresholdClear trap is generated.
low_thresh is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

Use this command to configure thresholds for the percentage of total DNS-learnt IP entries in relation to the ACS DNS Snooping feature. Note that this threshold applies to both IPv4 and IPv6 DNS entries.

Alerts or alarms are triggered based on the following rules:

- **Enter condition:** Actual percentage of total DNS-learnt IP entries is greater than or equal to the specified percentage of total DNS-learnt IP entries.
- **Clear condition:** Actual of total DNS-learnt IP entries is less than the specified clear percentage of total DNS-learnt IP entries.

If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval, and the **threshold monitoring ecs** command to enable thresholding for this value.

Example

The following command configures a high threshold of *65* percent and a clear threshold of *35* percent for total DNS-learnt IP entries:

```
threshold dns-learnt-ip-max-entries 65 clear 35
```

threshold edr-file-space

Configures the threshold for monitoring the percentage of total file space allocated for Event Data Records (EDRs) used during the polling interval.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

[default] threshold edr-file-space *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 90
Specifies the high threshold for percentage of total allocated EDR file space used that must be met or exceeded at the end of the polling interval to generate an alert or alarm.
high_thresh is measured in percentage of total allocated EDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold for percentage of total allocated EDR file space used that maintains a previously generated alarm condition. If the space usage falls below the low threshold within the polling interval, a clear alarm is generated.
low_thresh is measured in percentage of total allocated EDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

EDR file space usage generate alerts or alarms based on the percentage of total allocated EDR file space used during the polling interval.
Alerts or alarms are triggered for EDR file space usage session based on the following rules:

- **Enter condition:** Actual percentage of allocated EDR file space usage is greater than or equal to the specified percentage of total EDR file space.
- **Clear condition:** Actual EDR file space used is less than the specified clear percentage of total allocated EDR file space usage.

If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold of *65* percent and a clear threshold of *35* percent for of total allocated EDR file space usage:

```
threshold edr-file-space 65 clear 35
```

threshold edr-udr-dropped flow control

This command configures thresholds to monitor the total number of Event Data Records (EDRs) and Usage Data Records (UDRs) discarded due to flow control.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold edr-udr-dropped-flow-control *high_thresh* **[clear** *low_thresh* **]**

default threshold edr-udr-dropped-flow-control

default

Configures this command with the default threshold settings.
Default: High threshold: 90; Low threshold: 10

high_thresh

Specifies the high threshold for total number of EDRs + UDRs dropped due to flow control, which must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh must be an integer from 0 through 100000.
A value of 0 disables the threshold.
Default: 90

clear *low_thresh*

Specifies the low threshold for total number of EDRs + UDRs dropped that maintains a previously generated alarm condition. If the total number of EDRs + UDRs dropped falls below Specifies the low threshold within the polling interval, a clear alarm is generated.
low_thresh must be an integer from 0 through 100000 that must be lower than *high_thresh*.
A value of 0 disables the threshold.
Default: 10

Usage

Use this command to configure thresholds to monitor the total number of EDRs + UDRs discarded due to flow control. Alerts or alarms are generated based on the total number of EDRs + UDRs dropped during polling interval.
Alerts or alarms are triggered for EDR file space usage session based on the following rules:

- **Enter condition:** Actual number of EDRs + UDRs dropped greater than or equal to the specified number of EDRs + UDRs dropped.
- **Clear condition:** Actual number of EDR + UDRs dropped is less than the specified clear number of EDRs + UDRs dropped.

If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold of *90* and a clear threshold of *45* to monitor EDRs + UDRs dropped due to flow control:

```
threshold edr-udr-dropped-flow-control 90 clear 45
```

threshold fw-deny-rule

This command configures thresholds for Stateful Firewall Deny Rule.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

threshold fw-deny-rule *high_thresh* **[clear** *low_thresh* **]**

default threshold fw-deny-rule

default

Configures this command with the default threshold settings.
Default: 0—disabled

high_thresh

Specifies the Stateful Firewall Deny-Rule threshold value, which if met or exceeded generates an alert or alarm.
high_thresh must be an integer from 0 through 1000000.
Default: 0

clear *low_thresh*

Specifies the Stateful Firewall Deny-Rule alarm clear threshold value. If, in the same polling interval, the threshold falls below *low_thresh* a clear alarm is generated.
low_thresh must be an integer from 0 through 1000000.
Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

When the number of Deny-Rule exceeds a given value, a threshold is raised and it is cleared when the number of Deny-Rule fall below a value within the polling interval.
Refer to the **threshold poll** command to configure the polling interval, and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a Stateful Firewall Deny Rule high threshold of *1000* and a low threshold of *100* for a system using the Alarm Thresholding model:

```
threshold fw-deny-rule 1000 clear 100
```

threshold fw-dos-attack

This command configures thresholds for Stateful Firewall Denial-of-Service (DoS) attacks.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

threshold fw-dos-attack *high_thresh* **[clear** *low_thresh* **]**

default threshold fw-dos-attack

default

Configures this command with the default threshold settings.
Default: 0—disabled

high_thresh

Specifies the Stateful Firewall DoS attacks threshold value, which if met or exceeded generates an alert or alarm.
high_thresh must be an integer from 0 through 1000000.
Default: 0

clear *low_thresh*

Specifies the Stateful Firewall DoS attacks clear threshold value. If, in the same polling interval, the threshold falls below *low_thresh* a clear alarm is generated.
low_thresh must be an integer from 0 through 1000000.
Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

When the number of DoS attacks exceed a given value, a threshold is raised and it is cleared when the number of DoS attacks fall below a value within the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a Stateful Firewall DoS attacks high threshold of *1000* and a low threshold of *100* for a system using the Alarm Thresholding model:

```
threshold fw-dos-attack 1000 clear 100
```

threshold fw-drop-packet

This command configures thresholds for Stateful Firewall drop packets.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

threshold fw-drop-packet *high_thresh* **[clear** *low_thresh* **]**

default threshold fw-drop-packet

default

Configures this command with the default threshold settings.
Default: 0—disabled

high_thresh

Specifies the Stateful Firewall drop packets threshold value, which if met or exceeded generates an alert or alarm.
high_thresh must be an integer from 0 through 1000000.
Default: 0

clear *low_thresh*

Specifies the Stateful Firewall drop packets clear threshold value. If, in the same polling interval, the threshold falls below *low_thresh* a clear alarm is generated.
low_thresh must be an integer from 0 through 1000000.
Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

When the number of drop packets exceed a given value, a threshold is raised and it is cleared when the number of drop packets fall below a value within the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a Stateful Firewall drop packets high threshold of *1000* and a low threshold of *100* for a system using the Alarm thresholding model:

```
threshold fw-drop-packet 1000 clear 100
```

threshold fw-no-rule

This command configures thresholds for Stateful Firewall no rules.

Product

FW

Privilege

Security Administrator, Administrator

Syntax

threshold fw-no-rule *high_thresh* **[clear** *low_thresh* **]**

default threshold fw-no-rule

default

Configures this command with the default threshold settings.
Default: 0—disabled

high_thresh

Specifies the Stateful Firewall no rules threshold value, which if met or exceeded generates an alert or alarm.
high_thresh must be an integer from 0 through 1000000.
Default: 0

clear *low_thresh*

Specifies the Stateful Firewall no rules clear threshold value. If, in the same polling interval, the threshold falls below *low_thresh* a clear alarm is generated.
low_thresh must be an integer from 0 through 1000000.
Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

When the number of no rules exceed a given value, a threshold is raised and it is cleared when the number of no rules fall below a value within the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a Stateful Firewall no rules high threshold of *1000* and a low threshold of *100* for a system using the Alarm Thresholding model:

```
threshold fw-no-rule 1000 clear 100
```

threshold license

Configures thresholds for session license utilization by the system.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] threshold license remaining-sessions *low_thresh* **clear** *high_thresh*

remaining-sessions *low_thresh*

Default: 10
Specifies the low threshold session license utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
low_thresh is an integer from 0 through 100.

clear *high_thresh*

Default: 10
Specifies the high threshold session license utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated.
high_thresh is an integer from 0 through 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to Specifies the low threshold.

Usage

Session license utilization thresholds generate alerts or alarms based on the utilization percentage of all session capacity licenses during the specified polling interval.
The system uses session capacity license to dictate the maximum number of simultaneous sessions that can be supported. There are multiple session types that require licenses. Although, a single threshold is configured for all session types, alerts or alarms can be generated for each type.
Alerts or alarms are triggered for session license utilization based on the following rules:

- **Enter condition:** Actual session license utilization percentage per session type is greater than or equal to the low threshold.
- **Clear condition:** Actual session license utilization percentage per session type is greater than the high threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a session license low threshold percentage of *10* and a high threshold of *35* for a system using the Alarm thresholding model:

```
threshold license remaining-sessions 10 clear 35
```

threshold mgmt-cpu-memory-usage

Configures the thresholds for CPU memory usage.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold mgmt-cpu-memory-usage *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold percent of CPU memory usage that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is measured in percentage of total memory used and can be configured to an integer from 0 through 100. A value of 0 disables the threshold.

clear *low_thresh*

Specifies the low threshold percent of CPU memory usage that maintains a previously generated alarm condition. If the percentage falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is measured in percentage of total memory used and can be configured to an integer from 0 through 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

CPU memory usage thresholds generate alerts or alarms based on memory usage for the SMC CPU during the polling interval. A single threshold enables CPU monitoring for both the active and standby SMCs allowing for alerts or alarms to be generated for each CPU.
Alerts or alarms are triggered for SMC CPU memory usage based on the following rules:

- **Enter condition:** Actual CPU memory usage is greater than or equal to the high threshold
- **Clear condition:** Actual CPU memory usage is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Important: This command is not supported on all platforms.

Example

The following command configures a threshold of *65* percent of total SMC CPU memory usage and a clear threshold of *35* percent:

```
threshold mgmt-cpu-memory-usage 65 clear 35
```

threshold mgmt-cpu-utilization

Configures the thresholds for CPU utilization.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold mgmt-cpu-utilization *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold CPU utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 100.

clear *low_thresh*

Specifies the low threshold CPU utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

CPU utilization thresholds generate alerts or alarms based on the utilization percentage of each SMCCPU during the specified polling interval. Although, a single threshold is configured for both SMC CPUs, separate alerts or alarms can be generated for each CPU.
Alerts or alarms are triggered for SMC CPU utilization based on the following rules:

- **Enter condition:** Average measured CPU utilization for the last 5 minutes is greater than or equal to the high threshold.
- **Clear condition:** Average measured CPU utilization for the last 5 minutes is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Important: This command is not supported on all platforms.

Example

The following command configures a high threshold SMC CPU utilization percentage of *90* for a system using the Alert thresholding model:

```
threshold mgmt-cpu-utilization 90
```

threshold mme-attach-failure

Use this command to configure thresholds for the total number of MME Attach Failure messages to count across all the MME services in the system as threshold limit to generate alert or alarm.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

threshold total-mme-attach-failure *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0 (Disabled)
Specifies the high threshold number of total MME Attach Failure messages across all services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh can be configured to an integer from 0 through 100000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0 (Disabled)
Specifies the low threshold number of total MME Attach Failure messages across all services on a system that maintains a previously generated alarm condition. If the number of MME Attach Failure messages across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 100000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to monitor and set alarms or alerts when the total number of MME Attach Failure message across all the MME services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of MME Attach Failure message based on the following rules:

- **Enter condition:** Actual total number of MME Attach Failure messages is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of MME Attach Failure messages is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll mme-attach-failure** command to configure the polling interval and the **threshold monitoring mme-service** command to enable thresholding for this value.

Example

The following command configures the limit of MME Attach Failure high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold mme-attach-failure 10000
```

threshold mme-auth-failure

Use this command to configure thresholds for the total number of MME Auth Failure messages to count across all the MME services in the system as threshold limit to generate alert or alarm.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

threshold total-mme-auth-failure *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0 (Disabled)
Specifies the high threshold number of total MME Auth Failure messages across all MMM services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh can be configured to an integer from 0 through 100000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0 (Disabled)
Specifies the low threshold number of total MME Auth Failure messages across all services on a system that maintains a previously generated alarm condition. If the number of MME Attach Failure messages across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 100000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to monitor and set alarms or alerts when the total number of MME Auth Failure message across all the MME services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of MME Auth Failure message based on the following rules:

- **Enter condition:** Actual total number of MME Auth Failure messages is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of MME Auth Failure messages is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll mme-auth-failure** command to configure the polling interval and the **threshold monitoring mme-service** command to enable thresholding for this value.

Example

The following command configures a total MME Auth Failure high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold mme-auth-failure 10000
```

threshold model

Configures the thresholding model for the system to use.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
threshold model { alarm | alert }
```

alarm

Selects the alarm thresholding model as described in the *Usage* section for this command.

alert

Selects the alert thresholding model as described in the *Usage* section for this command.

Usage

The system supports the following thresholding models:

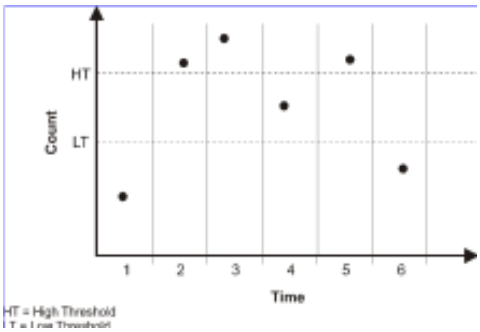
- **Alert:** A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

In the example shown in the figure below, this model generates alerts during period 2, 3, and 5 at the point where the count exceeded the high threshold.

- **Alarm:** Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

The alarm is cleared at the end of the first interval where the measured value is below the low threshold. In the example shown in the figure below, this model generates an alarm during period 2 when the count exceeds the high threshold. A second alarm is generated in period 6 when the count falls beneath low threshold. The second alarm indicates a "clear" condition.

Figure 4. Thresholding Model Example



Important: For certain values the alert or alarm serves to warn of low quantities (such as, memory, session licenses, etc.). In these cases, the low threshold is the condition that must be met or exceeded within the polling interval to generate the alert or alarm. When the high threshold is exceeded during an interval, the low quantity condition is cleared.

Refer to the **`threshold monitoring`** command for additional information on thresholding.

Example

The following command configures the system to support the Alarm thresholding model:

```
threshold model alarm
```

threshold monitoring

Enables thresholding for the selected value.

Product

All

Privilege

Administrator

Syntax

[no | default] threshold monitoring { aaa-acct-archive-queue | aaa-acct-archive-size | aaa-acct-failure | aaa-auth-failure | aaa-retry-rate | aaamgr-request-queue | asngw | call-setup | content-filtering | cpu-resource | cpu-session-throughput | diameter | ecs | fa-service | firewall | ha-service | hnbgw-service | hsgw-service | ipsec | license | lma-service | mme-service | packets-filtered-dropped | packets-forwarded-to-cpu | pdsn-service | pdg-service | pdif-service | pgw-service | route-service | sgw-service | subscriber | system | tpo }

no

Disables threshold monitoring for the specified value.

default

Sets or restores the default value assigned to the specified parameter.

aaa-acct-archive-queue

Enables threshold monitoring for the AAA accounting archive message queue size.
Refer to the **threshold aaa-acct-archive-queue-size** command for additional information on these values.

aaa-acct-archive-size

Enables threshold monitoring for the size of the AAA accounting record archive.

aaa-acct-failure

Enables threshold monitoring for AAA accounting failures and AAA accounting failure rate values.
Refer to the **threshold aaa-acct-failure** and **threshold aaa-acct-failure-rate** commands for additional information on these values.

aaa-auth-failure

Enables threshold monitoring for AAA authentication failures and AAA authentication failure rate values.
Refer to the **threshold aaa-auth-failure** and **threshold aaa-auth-failure-rate** commands for additional information on these values.

aaa-retry-rate

Enables threshold monitoring for the AAA retry rate value.
Refer to the **threshold aaa-retry-rate** command for additional information on this value.

aaamgr-request-queue

Enables threshold monitoring for AAA Manager Requests for each AAA manager process. Refer to the **threshold aaamgr-request-queue** command for additional information on these values.

asngw

Enables the threshold monitoring for ASN-GW services.

call-setup

Enables threshold monitoring for the call setup, call setup failures, and no-resource rejected call values.
Refer to the **threshold call-setup, threshold call-setup-failure, threshold ppp-setup-fail-rate, threshold rp-setup-fail-rate**, and **threshold call-reject-no-resource** commands for additional information on these values.

cpu-resource

Enables threshold monitoring for CPU thresholds.
Refer to the **threshold 10sec-cpu-utilization, threshold cpu-available-memory, threshold cpu-load, threshold cpu-memory-usage, threshold cpu-orbs-crit, threshold cpu-orbs-warn, threshold cpu-session-throughput, threshold cpu-utilization, threshold mgmt-cpu-memory-usage**, and **threshold mgmt-cpu-utilization** commands for additional information on these values.

cpu-session-throughput

Enables threshold monitoring for the CPU session throughput value.
Refer to the **threshold cpu-session-throughput** command for additional information on this value.

content-filtering

Enables threshold monitoring for the Content Filtering in-line service.

diameter

Enables threshold monitoring for Diameter.

ecs

Enables threshold monitoring for the Active Charging Service (ACS)/Enhanced Charging Service (ECS).

fa-service

Enables threshold monitoring for Registration Reply errors for each FA service.
Refer to the **threshold reg-reply-error** FA Service Configuration Mode command for additional information on this value.

firewall

Enables threshold monitoring for the Stateful Firewall in-line service.
Default: Disabled
Refer to the **threshold fw-deny-rule, threshold fw-dos-attack, threshold fw-drop-packet**, and **threshold fw-no-rule** commands for additional information on this value.

Important: Stateful Firewall thresholds can only be enabled if the Stateful Firewall license is present.

ha-service

Enables threshold monitoring for Registration Reply errors, re-registration reply errors, deregistration reply errors, and average calls setup per second for each HA service and average calls setup per second at the context level.
Refer to the **threshold init-rrq-rcvd-rate, threshold reg-reply-error, threshold rereg-reply-error,** and **threshold dereg-reply-error** HA Service Configuration Mode commands and the **threshold ha-service init-rrq-rcvd-rate** Context Configuration mode command for additional information on this value.

hnbgw-service

Enables threshold monitoring for HNB-GW sessions including Iu-CS and Iu-PS sessions for HNB-GW services on a system at the system level.

Important: This keyword is required to activate the threshold alarm/alert for HNB-GW service to use **threshold total-hnbgw-hnb-sessions**, **thresshold total-hnbgw-iu-sessions**, and **thresshold total-hnbgw-ue-sessions** command for threshold values.

hsgw-service

Enables threshold monitoring for HSGW services.
Refer to the threshold total-hsgw-sessions for more information on HSGW thresholds.

ipsec

Enables monitoring of IPSec thresholds.
refer to the HA-Service Configuration Mode chapter of the Command Line Interface Reference for information on the IPSec thresholds.

license

Enables threshold monitoring for the session license value.
Refer to the **threshold license** command for additional information on this value.

lma-service

Enables threshold monitoring for LMA services.
Refer to the threshold total-lma-sessions for more information on LMA thresholds.

mme-service

Default: Disabled.
Enables threshold monitoring for the MME services.
Refer to the t**hreshold total-mme-sessions** commands for additional information on this value.

packets-filtered-dropped

Enables threshold monitoring for the filtered/dropped packet value.
Refer to the **threshold packets-filtered-dropped** command for additional information on this value.

packets-forwarded-to-cpu

Enables threshold monitoring for the forwarded packet value.
Refer to the **threshold packets-forwarded-to-cpu** command for additional information on this value.

pdg-service

Enables threshold monitoring for PDG service.
Threshold monitoring for PDG service is disabled by default.

pdif-service

Enables threshold monitoring for PDIF service.

pdsn-service

Enables threshold monitoring for average calls setup per second for contexts and for PDSN services, A11 Request.
Refer to the **threshold packets-forwarded-to-cpu** command for additional information on this value.

pgw-service

Enables threshold monitoring for P-GW services.
Refer to the threshold total-pgw-sessions for more information on P-GW thresholds.

route-service

Enables threshold monitoring for BGP/VRF route services.
Refer to the **ip maximum-routes** command in Context configuration mode and **threshold route-service bgp-routes** in this mode for more information on route thresholds.

sgw-service

Enables threshold monitoring for S-GW services.
Refer to the threshold total-sgw-sessions for more information on S-GW thresholds.

subscriber

Enables threshold monitoring for the subscriber and session values.
Refer to the **threshold subscriber active**, **threshold subscriber total**, **threshold total-ggsn-sessions**, **threshold total-gprs-sessions**, **threshold total-gprs-pdp-sessions**, **threshold total-ha-sessions**, **threshold total-lns-sessions**, **threshold total-pdsn-sessions**, **threshold total-sgsn-sessions**, **threshold total-sgsn-pdp-sessions**, **threshold per-service-ggsn-sessions**, **threshold per-service-ha-sessions**, t**hreshold per-service-lns-sessions**, and **threshold per-service-pdsn-sessions** commands for additional information on these values.

system

Enables system (chassis) thresholds monitoring.

tpo

Enables thresholds monitoring for Traffic Performance Optimization (TPO) in-line service.

Usage

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the SNMP MIB Reference.

The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.
- **Alarm System:** High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists and/or a condition clear alarm is generated.

"Outstanding" alarms are reported to through the system's alarm subsystem and are viewable through the CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

Table 22. Thresholding Reporting Mechanisms by Model

Model	SNMP Traps	Logs	Alarm System
Alert	X	X	
Alarm	X	X	X

In addition to the values that can be enabled by this command, the system supports the enabling of threshold monitoring for IP pool address availability (refer to the **ip pool** and threshold commands in this reference) and port utilization (refer to the threshold commands in this chapter).

Example

The following command enables thresholding for subscriber totals:

```
threshold monitoring subscriber
```

threshold nat-port-chunks-usage

This command configures the Network Address Translation (NAT) port chunk utilization threshold settings.

Important: This command is only available in 8.3 and later releases.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

threshold nat-port-chunks-usage *high_thresh* **[clear** *low_thresh* **]**

default threshold nat-port-chunks-usage

default

Configures this command with the default threshold settings.
Default: 0—disabled

high_thresh

Specifies the high NAT-port-chunks-usage percentage threshold that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh must be an integer from 0 through 100. A value of 0 disables the threshold.
Default: 0

clear *low_thresh*

Specifies the low nat-port-chunks-usage percentage threshold that must be met within the polling interval for a clear alarm to be generated.
low_thresh must be an integer from 0 through 100. A value of 0 disables the threshold. If not set, the *high_thresh* will be the high and low threshold setting.
Default: 0

Usage

Use this command to configure the NAT port chunk utilization threshold settings.

Example

The following command sets the NAT port chunk utilization threshold settings to a high of *75*% and a low of *15*%:

```
threshold nat-port-chunks-usage 75 clear 15
```

threshold packets-filtered-dropped

Configures filtered or dropped packet thresholds for the system.

Product

PDSN, GGSN, HA, SGSN, ASN GW

Privilege

Security Administrator, Administrator

Syntax

threshold packets-filtered-dropped *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of filtered/dropped packets experienced by the system resulting from access control list (ACL) rules that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 1000000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of filtered/dropped packets experienced by the system resulting from ACL rules that maintains a previously generated alarm condition. If the number of packets falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 1000000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Filtered/dropped packet thresholds generate alerts or alarms based on the total number of packets that were filtered or dropped by the system as a result of ACL rules during the specified polling interval.
Alerts or alarms are triggered for filtered/dropped packets based on the following rules:

- **Enter condition:** Actual number of filtered/dropped packets is greater than or equal to the high threshold.
- **Clear condition:** Actual number of filtered/dropped packets is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value. In addition, refer to information on ACLs in this reference.

Example

The following command configures a filtered/dropped packet high threshold count of *150000* for a system using the Alert thresholding model:

```
threshold packets-filtered-dropped 150000
```

threshold packets-forwarded-to-cpu

Configures forwarded packet thresholds for the system.

Product

PDSN, GGSN, HA, SGSN, ASN GW

Privilege

Security Administrator, Administrator

Syntax

threshold packets-forwarded-to-cpu *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of forwarded packets experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 1000000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of forwarded packets experienced by the system that maintains a previously generated alarm condition. If the number of packets falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 1000000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Forwarded packet thresholds generate alerts or alarms based on the total number of packets that were forwarded to active system CPU(s) during the specified polling interval. Packets are forwarded to active system CPUs when the NPUs do not have adequate information to properly route them.

Important: Ping and/or traceroute packets are intentionally forwarded to system CPUs for processing. These packet types are included in the packet count for this threshold.

Alerts or alarms are triggered for forwarded packets based on the following rules:

- **Enter condition:** Actual number of forwarded packets is greater than or equal to the high threshold
- **Clear condition:** Actual number of forwarded packets is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a forwarded packet high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold packets-forwarded-to-cpu 10000
```

threshold pdg-current-active-sessions

Configures the threshold for monitoring the total number of all current Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) sessions only.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

threshold pdg-current-active-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Configures the total number of active PDG sessions to be monitored on a chassis. *high_thresh* is an integer from 0 through 300000.
There is no default, but 0 means that there is no threshold monitoring.

clear *low_thresh*

Clears the number of sessions being monitored using the *high_thresh* variable defined above. *low_thresh* is an integer from 0 through 100000.

Usage

Thresholds are provided for monitoring the overall PDG usage on a chassis. This command is used to monitor the total number of active PDG sessions for an entire chassis.

Example

The following command configures a monitoring threshold of *300000* active PDG sessions on a chassis:

```
threshold pdg-current-active-sessions 300000
```

which turns out to be too many, so the following command clears *100000*:

```
threshold pdg-current-active-sessions 300000 clear 100000
```

threshold pdg-current-sessions

Configures the threshold for monitoring the total number of all current Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) sessions, including inactive sessions.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

threshold pdg-current-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Configures the total number of PDG sessions on a chassis, both active and inactive. *high_thresh* is any integer from 0 through 300000.
There is no default, but 0 means that there is no threshold monitoring.

clear *low_thresh*

Clears any number of sessions being monitored using the *high_thresh* variable defined above. *low_thresh* is any integer from 0 through 100000.

Usage

Thresholds are provided for monitoring the overall PDG usage on a chassis. This command is used to monitor the total number of PDG sessions, both active and inactive, for an entire chassis.

Example

The following command configures a monitoring threshold of *300000* active and inactive PDG sessions on a chassis:

```
threshold pdg-current-sessions 300000
```

which turns out to be too many, so the following command clears *100000*:

```
threshold pdg-current-sessions 300000 clear 100000
```

threshold pdif-current-sessions

Configures the threshold for monitoring the total number of all current Packet Data Interworking Function (PDIF) sessions, including inactive sessions.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

threshold pdif-current-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Configures the total number of PDIF sessions on a chassis, both active and inactive. *high_thresh* is an integer from 0 through 1000000.
There is no default, but 0 means that there is no threshold monitoring.

clear *low_thresh*

Clears the specified number of sessions being monitored using the *high_thresh* variable defined above. *low_thresh* is an integer from 0 through 1000000.

Usage

Thresholds are provided for monitoring the overall PDIF usage on a chassis. This command is used to monitor the total number of PDIF sessions, both active and inactive, for an entire chassis.

Example

The following command configures a monitoring threshold of *300000* active and inactive PDIF sessions on a chassis:

```
threshold pdif-current-sessions 300000
```

which turns out to be too many, so the following command clears *100000*:

```
threshold pdif-current-sessions 300000 clear 100000
```

threshold pdif-current-active-sessions

Configures the threshold for monitoring the total number of current Packet Data Interworking Function (PDIF) sessions only.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

threshold pdif-current-active sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Configures the total number of active PDIF sessions to be monitored on a chassis. *high_thresh* is any integer from 0 through 1000000.
There is no default, but 0 means that there is no threshold monitoring.

clear *low_thresh*

Clears the specified number of sessions being monitored using the *high_thresh* variable defined above. *low_thresh* is any integer from 0 through 1000000.

Usage

Thresholds are provided for monitoring the overall PDIF usage on a chassis. This command is used to monitor the total number of active PDIF sessions for an entire chassis.

Example

The following command configures a monitoring threshold of *300000* active PDIF sessions on a chassis:

```
threshold pdif-current-active-sessions 300000
```

which turns out to be too many, so the following command clears *100000*:

```
threshold pdif-current-active-sessions 300000 clear 100000
```

threshold per-service-ggsn-sessions

Configures thresholds for the number of PDP contexts per GGSN service in the system.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

threshold per-service-ggsn-sessions *high_thresh* **[** *clear low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of PDP contexts for any one GGSN service that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of PDP contexts for any one GGSN service that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the number of PDP contexts for any GGSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of PDP contexts for any GGSN service is greater than or equal to the high threshold
- **Clear condition:** Actual number of PDP contexts is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *10000* subscriber attaches per GGSN service for the Alert thresholding model:

```
threshold per-service-ggsn-sessions 10000
```

threshold per-service-gprs-pdp-sessions

Configures thresholds for the number of 2G-activated PDP contexts per GPRS service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

threshold per-service-gprs-pdp-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of 2G-activated PDP contexts for any one GPRS service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of 2G-activated PDP contexts for any one GPRS service. This number or higher maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, then a clear alarm will be generated.
low_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the number of 2G-activated PDP contexts for any GPRS service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of PDP contexts for any GPRS service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of PDP contexts is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *10000* 2G-activated PDP contexts per GPRS service for the Alert thresholding model:

```
threshold per-service-gprs-sessions 10000
```

threshold per-service-gprs-sessions

Configures the thresholds for the number of 2G-attached subscribers per GPRS service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

threshold per-service-gprs-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of 2G-attached subscribers for any one GPRS service. This threshold number must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 2000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of 2G-attached subscribers for any one GPRS service. The number of subscribers must remain above this threshold in order to maintain a previously generated alarm condition. If the number of 2G subscribers falls beneath the low threshold within the polling interval, then a clear alarm will be generated.
low_thresh is an integer from 0 through 2000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the number of 2G-attached subscribers for any GPRS service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of 2G-attached subscribers for any GPRS service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of 2G-attached subscribers is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *10000* 2G-attaches per GPRS service for the Alert thresholding model:

```
threshold per-service-gprs-sessions 10000
```

threshold per-service-ha-sessions

Configures thresholds for the number of HA sessions per HA service in the system.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

threshold per-service-ha-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of HA sessions for any one HA service that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 500000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of HA sessions for any one HA service that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 500000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the number of HA sessions for any HA service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for HA sessions based on the following rules:

- **Enter condition:** Actual number of HA sessions for any HA service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of HA sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a HA session per service high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold per-service-ha-sessions 10000
```

threshold per-service-lns-sessions

Configures thresholds for the number of L2TP Network Server (LNS) sessions per LNS service in the system.

Product

PDSN, GGSN, HA, ASN GW

Privilege

Security Administrator, Administrator

Syntax

threshold per-service-lns-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of LNS sessions for any one LNS service that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 500000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of LNS sessions for any one LNS service that maintains a previously generated alarm condition. If the number of LNS sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 500000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the number of LNS sessions for any LNS service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for LNS sessions based on the following rules:

- **Enter condition:** Actual number of LNS sessions for any LNS service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of LNS sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a LNS session per service high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold per-service-lns-sessions 10000
```

threshold per-service-pdsn-sessions

Configures thresholds for the number of Packet Data Serving Node (PDSN) sessions per PDSN service in the system.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

threshold per-service-pdsn-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of PDSN sessions for any one PDSN service that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 500000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of PDSN sessions for any one PDSN service that maintains a previously generated alarm condition. If the number of PDSN sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 500000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the number of PDSN sessions for any PDSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDSN sessions based on the following rules:

- **Enter condition:** Actual number of PDSN sessions for any PDSN service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of PDSN sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a HA session per service high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold per-service-pdsn-sessions 10000
```

threshold per-service-sgsn-pdp-sessions

Configures the thresholds for the number of 3G-activated PDP contexts per SGSN service on the system.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

threshold per-service-sgsn-pdp-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of 3G-activated PDP contexts for any one SGSN service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of 3G-activated PDP contexts for any one SGSN service. This number or higher maintains a previously generated alarm condition. If the number of 3G-activated PDP contexts falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 2400000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the number of 3G-activated PDP contexts for any SGSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of 3G-activated PDP contexts for any SGSN service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of 3G-activated PDP contexts is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *10000* 3G-activated PDP contexts per SGSN service for the system's Alert thresholding model:

```
threshold per-service-sgsn-sessions 10000
```

threshold per-service-sgsn-sessions

Configures the thresholds for the number of 3G-attached subscribers per SGSN service in the system.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

threshold per-service-sgsn-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of 3G-attached subscribers for any one SGSN service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 2000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of 3G-attached subscribers for any one SGSN service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 2000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the number of 3G-attached subscribers for any one SGSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of 3G-attached subscribers for any single SGSN service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of 3G-attached subscribers for any single SGSN service is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold count of *10000* 3G-attached subscribers per SGSN service for a system using the Alert thresholding model:

```
threshold per-service-sgsn-sessions 10000
```

threshold poll

This command configures the polling interval over which to count or measure the thresholding value.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[default] threshold poll { 10sec-cpu-utilization | all-ppp-send-discard | a11-rac-msg-discard |a11-rrp-failure | a11-rrq-msg-discard | aaa-acct-archive-queue-size1 | aaa-acct-archive-queue-size2 | aaa-acct-archive-queue-size3 aaa-acct-archive-size | aaa-acct-failure | aaa-acct-failure-rate | aaa-auth-failure | aaa-auth-failure-rate | aaa-retry-rate | aaamgr-request-queue | active-subscriber | asngw-auth-failure | asngw-handoff-denial | asngw-max-eap-retry | asngw-network-entry-denial | asngw-session-setup-timeout | asngw-session-timeout | asnpc-idle-mode-timeout | asnpc-im-entry-denial | asnpc-lu-denial | asnpc-session-setup-timeout | available-ip-pool-group | call-reject-no-resource | call-setup | call-setup-failure | call-setup-failures | call-total-active | cdr-file-space | contfilt-block | contfilt-rating | cpu-available-memory | cpu-load | cpu-memory-usage | cpu-orbs-crit | cpu-orbs-warn | cpu-session-throughput | cpu-utilization | cscf-invite-rcvd | cscf-reg-rcvd | cscf-service-route-failures | dcca-bad-answers | dcca-protocol-error | dcca-rating-failed | dcca-unknown-rating-group | dereg-reply-error | | diameter-retry-rate | edr-file-space | edr-udr-dropped-flow-control | error-no-resource| error-presence | error-reg-auth | error-tcp| fa-reg-reply-error | fng-current-active-sessions | fng-current-sessions | fw-deny-rule | fw-dos-attack | fw-drop-packet | fw-no-rule | ha-init-rrq-rcvd-rate | ha-svc-init-rrq-rcvd-rate | ip-pool-free | ip-pool-hold | ip-pool-release | ip-pool-used | ipsec-call-req-rej | ipsec-ike-failrate | ipsec-ike-failures | ipsec-ike-requests | ipsec-tunnels-established | ipsec-tunnels-setup | license-remaining-session | mgmt-cpu-memory-usage interval | mgmt-cpu-utilization | nat-port-chunks-usage | packets-filtered-dropped | packets-forwarded-to-cpu | pdg-current-active-sessions | pdg-current-sessions | pdif-current-active-sessions | pdif-current-sessions | pdsn-init-rrq-rcvd-rate | pdsn-svc-init-rrq-rcvd-rate | per-service-asngw-sessions | per-service-ggsn-sessions | per-service-gprs-sessions | per-service-gprs-pdp-sessions | per-service-ha-sessions | per-service-lns-sessions | per-service-pdsn-sessions | per-service-sgsn-sessions | per-service-sgsn-pdp-sessions | port-high-activity | port-rx-utilization | port-tx-utilization | ppp-setup-fail-rate | reg-reply-error | reg-total-active | rereg-reply-error | route-service | rp-setup-fail-rate | storage-utilization total-asngw-sessions | total-ggsn-sessions | total-gprs-sessions | total-gprs-pdp sessions | total-ha-sessions | total-hsgw-sessions | total-lma-sessions | total-lns-sessions | total-mme-sessions | total-pdsn-sessions | total-pgw-sessions | total-sgsn-sessions | total-sgsn-pdp-sessions | total-sgw-sessions | total-subscriber } interval *time*

default

Restores the specified parameter to its default value.

10sec-cpu-utilization percent

Default: 300 seconds (5 minutes)
Configures the polling interval for measuring a 10-second average of CPU utilization.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

a11-rrp-failure

Default: 0
Configures the polling interval over which to count A11 Registration Response failures. When specifying **interval** *time* for this threshold, the range is from 60 through 900 seconds.

a11-rrq-msg-discard

Default: 0
Configures the polling interval over which to count how many A11 Registration Request messages are discarded. When specifying **interval** *time* for this threshold, the range is from 60 through 900 seconds.

a11-rac-msg-discard

Default: 0
Configures the polling interval over which to count how many A11 Registration Acknowledgement messages are discarded. When specifying **interval** *time* for this threshold, the range is from 60 through 900 seconds.

aaa-acct-archive-queue-size1

Default: 900 seconds (15 minutes)
Configures the polling interval over which to measure AAA accounting archive message queue size.

aaa-acct-archive-queue-size2

Default: 900 seconds (15 minutes)
Configures the polling interval over which to measure AAA accounting archive message queue size.

aaa-acct-archive-queue-size3

Default: 900 seconds (15 minutes)
Configures the polling interval over which to measure AAA accounting archive message queue size.

aaa-acct-archive-size

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count archived AAA accounting messages.

aaa-acct-failure

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count failed AAA accounting requests.

aaa-acct-failure-rate

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of AAA accounting failures.

aaa-auth-failure

Default: 300 seconds (5 minutes)

Configures the polling interval over which to count failed authentication requests.

aaa-auth-failure-rate

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of AAA authentication failures.

aaa-retry-rate

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percent of AAA request message retries.

aaamgr-request-queue

Default: 0
Configures the polling interval over which to count the number of AAA Manager Requests for each AAA manager process. When specifying **interval** *time* for this threshold, the range is from 60 through 60000 seconds.

active-subscriber

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of active subscriber sessions.

all-ppp-send-discard

Default: 0
Configures the polling interval over which to count the number of discarded PPP send packets. When specifying **interval** *time* for this threshold, the range is from 60 through 900 seconds.

available-ip-pool-group

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure IP pool utilization.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

call-reject-no-resource

Default: 900 seconds (15 minutes)
Configures the polling interval over which to count the number of calls rejected due to insufficient resources.

call-setup

Default: 900 seconds (15 minutes)
Configures the polling interval over which to count the number of calls setup.

call-setup-failure

Default: 900 seconds (15 minutes)
Configures the polling interval over which to count the number of calls setup failures.

call-setup-failures

Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count CSCF call setup failures.
time must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

call-total-active

Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count CSCF total active calls.
time must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

cpu-available-memory

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure packet processing card CPU memory availability.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

Important: This command is not supported on all platforms

cpu-load

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure packet processing card CPU load using a 5-minute average measurement.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

Important: This command is not supported on all platforms

cpu-memory-usage

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of total packet processing card CPU memory used.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

Important: This command is not supported on all platforms

cpu-orbs-crit

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of CPU utilization by the ORBS software task for critical-level alerts.

cpu-orbs-warn

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of CPU utilization by the ORBS software task for warning-level alerts.

cpu-session-throughput

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure packet processing card CPU session throughput.

Important: This command is not supported on all platforms

cpu-utilization

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure packet processing card CPU utilization.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

Important: This command is not supported on all platforms

cscf-invite-rcvd

Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count the Call State Control Function (CSCF) calls. *time* must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

cscf-reg-rcvd

Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count the CSCF registrations.
time must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

cscf-service-route-failures

Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count the CSCF service route failures.
time must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

dcca-bad-answers

Configures the polling interval in seconds over which to count Diameter bad answers.

dcca-protocol-error

Configures the polling interval in seconds over which to count Diameter protocol errors.

dcca-rating-failed

Configures the polling interval in seconds over which to count Diameter rating failures.

dcca-unknown-rating-group

Configures the polling interval in seconds over which to count Diameter unknown rating group errors.

dereg-reply-error

Default: 0
Configures the polling interval over which to measure the number of de-registration reply errors for HA services. When specifying **interval** *time* for this threshold, the range is from 60 through 900 seconds.

diameter-retry-rate

Configures the polling interval over which to measure the number of retries to Diameter server. When specifying **interval** *time* for this threshold, the range is from 60 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30.

edr-file-space

Configures the polling interval in seconds over which to count Event Data Record (EDR) file space.

edr-udr-dropped-flow-control

Configures the polling interval in seconds over which to count EDR-UDRs Dropped due to Flow Control at ACSMGR.

error-no-resource

Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count CSCF No Resource Errors.
time must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

error-presence

Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count CSCF Presence Errors.
time must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

error-reg-auth

Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count CSCF Reg-Auth Errors.
time must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

error-tcp

Default: 300 seconds (5 minutes)
Configures the polling interval in seconds over which to count CSCF TCP Errors.
time must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

fa-reg-reply-error

Default: 0
Configures the polling interval over which to measure the number of registration reply errors for FA services. When specifying **interval** *time* for this threshold, the range is from 60 through 900 seconds.

fng-current-active-sessions

Configures the polling interval in seconds over which to count FNG current active sessions.

fng-current-sessions

Configures the polling interval in seconds over which to count FNG current sessions.

fw-deny-rule

Default: 900 seconds (15 minutes)
Configures the Stateful Firewall Deny-Rule threshold polling interval. For this threshold the interval time range is from 60 through 900 seconds.

fw-dos-attack

Default: 900 seconds (15 minutes)
Configures the Stateful Firewall DoS-Attacks threshold polling interval. For this threshold the interval time range is from 60 through 900 seconds.

fw-drop-packet

Default: 900 seconds (15 minutes)
Configures the Stateful Firewall Drop-Packet threshold polling interval. For this threshold the interval time range is from 60 through 900 seconds.

fw-no-rule

Default: 900 seconds (15 minutes)
Configures the Stateful Firewall No-Rule threshold polling interval. For this threshold the interval time range is from 60 through 900 seconds.

ha-init-rrq-rcvd-rate

Default: 0
Configures the polling interval over which to measure the average number of calls setup per minute for the context. When specifying **interval** *time* for this threshold, the range is from 60 through 900 seconds.

ha-svc-init-rrq-rcvd-rate

Default: 0
Configures the polling interval over which to measure the average number of calls setup per minute for HA services. When specifying **interval** *time* for this threshold, the range is from 60 through 900 seconds.

ip-pool-free

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of the IP pool addresses that are in the free state.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

ip-pool-hold

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of the IP pool address that are in the hold state.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

ip-pool-release

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of IP pool address that are in the release state.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

ip-pool-used

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure the percentage of the IP pool addresses that are used.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

ipsec-ipsec-call-req-rej

Default: 900
Configures the polling interval over which to count the IPSec call requests that are rejected.

ipsec-ike-failrate

Default: 900
Configures the polling interval over which to count the IPSec IKE failure rate.

ipsec-ike-failures

Default: 900
Configures the polling interval over which to count the IPSec IKE failures.

ipsec-ike-requests

Default: 900
Configures the polling interval over which to count the IPSec IKE request.

ipsec-tunnels-established

Default: 900
Configures the polling interval over which to count the IPSec tunnels established.

ipsec-tunnels-setup

Default: 900
Configures the polling interval over which to count the IPSec tunnels setup.

license-remaining-session

Default: 900 seconds (15 minutes)
Configures the polling interval over which to measure session license utilization.

mgmt-cpu-memory-usage interval

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure SMC CPU memory usage.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

Important: This command is not supported on all platforms

mgmt-cpu-utilization

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure SMC CPU usage.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

Important: This command is not supported on all platforms.

nat-port-chunks-usage

Important: This keyword is only available in 8.3 and later releases.

Default: 900 seconds (15 minutes)
Configures the polling interval over which to measure NAT port chunks usage.

packets-filtered-dropped

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the filtered/dropped packets.

packets-forwarded-to-cpu

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the forwarded packets.

pdg-current-active-sessions

Configures how frequently the system polls the pdg-current-active-sessions threshold.

pdg-current-sessions

Configures how frequently the system polls the pdg-current-sessions threshold.

threshold poll pdif-current-sessions interval *period*

Configures the polling interval for all current PDIF sessions in seconds rounded to the nearest multiple of 30 seconds. *period* is an integer from 30 to 60000.

threshold poll pdif-current-active-sessions interval *period*

Configures the polling interval for active sessions only in seconds rounded to the nearest multiple of 30 seconds. *period* is an integer from 30 to 60000.

pdsn-init-rrq-rcvd-rate

Default: 0
Configures the polling interval over which to measure the average number of calls setup per second for a PDSN-service. When specifying **interval** *time* for this threshold, the range is from 60 through 900 seconds.

pdsn-svc-init-rrq-rcvd-rate

Configures the polling interval in seconds over which to count PDSN per-service call received rate.

per-service-asngw-sessions

Configures the polling interval in seconds over which to count per service ASN-GW sessions.

per-service-ggsn-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the number of PDP contexts per GGSN service.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

per-service-gprs-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval during which the SGSN counts the number of 2G-attached subscriber per GPRS service.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

per-service-gprs-pdp-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval during which the SGSN counts the number of 2G-activated PDP contexts per GPRS service.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

per-service-ha-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the number of HA sessions per HA service.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

per-service-lns-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the number of L2TP Network Server (LNS) sessions per LNS service.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

per-service-pdsn-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the number of PDSN sessions per PDSN service.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

per-service-sgsn-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval during which the SGSN counts the number of 3G-attached subscribers per SGSN service.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

per-service-sgsn-pdp-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval during which the SGSN counts the number of 3G-activated PDP contexts per SGSN service.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

port-high-activity

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure for high port activity.

Important: This command is not supported on all platforms

port-rx-utilization

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure receive port utilization.

Important: This command is not supported on all platforms

port-tx-utilization

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure transmit port utilization.

Important: This command is not supported on all platforms

ppp-setup-fail-rate

Default: 900 seconds (15 minutes)
Configure the polling interval over which to measure the PPP setup failure rate.

reg-reply-error

Default: 0

Configures the polling interval over which to measure number of registration reply errors for HA services. When specifying **interval** *time* for this threshold, the range is from 60 through 900 seconds.

reg-total-active

Default: 300 seconds (5 minutes)
Configures the polling interval over which to measure CSCF Total Active Registrations.
time must an integer value from 60 to 60000 and expressed in multiples of 30. The system will round up all other configured values to a multiple of 30.

rereg-reply-error

Default: 0
Configures the polling interval over which to measure number of re-registration reply errors for HA services. When specifying **interval** *time* for this threshold, the range is from 60 through 900 seconds.

rp-setup-fail-rate

Default: 900 seconds (15 minutes)
Configure the polling interval over which to measure the RP setup failure rate.

spc-cpu-memory-usage interval

Important: This command has been renamed to **threshold mgmt-cpu-memory-usage**. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.

Important: This command is not supported on all platforms

spc-cpu-utilization

Important: This command has been renamed to **threshold mgmt-cpu-utilization**. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.

Important: This command is not supported on all platforms

storage-utilization

Default: 900 seconds (15 minutes)
Configures the polling interval over which to record the CompactFlash utilization percentage threshold interval in seconds.

total-asngw-sessions

Configures the polling interval over which to measure total ASN-GW sessions on the system.

total-ggsn-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of GGSN sessions on the system.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

total-gprs-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of 2G-attached subscribers on the system.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

total-gprs-pdp-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of 2G-activated PDP contexts per GPRS sessions on the system.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

total-ha-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of HA sessions on the system.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

total-hsgw-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of HSGW sessions on the system.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

total-lma-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of Local Mobility Anchor (LMA) sessions on the system.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

total-lns-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of LNS sessions on the system.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

total-pdsn-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of PDSN sessions on the system.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

total-pgw-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of P-GW sessions on the system.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

total-sgsn-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of SGSN sessions on the system.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

total-sgsn-pdp-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of SGSN sessions on the system.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

total-sgw-sessions

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of S-GW sessions on the system.

Important: When specifying **interval** *time* for this threshold, the range is from 30 through 60000 seconds. If the value entered is not a multiple of 30, the value is automatically rounded up to the next highest multiple of 30. (If you enter 35, the value is rounded to 60.)

total-subscriber

Default: 300 seconds (5 minutes)
Configures the polling interval over which to count the total number of subscriber sessions.

interval *time*

Specifies the amount of time that comprises the polling interval.
time is measured in seconds and can be configured to any integer value from 60 to 60000 unless otherwise noted in keyword descriptions.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.

Example

The following command configures the polling interval for the total subscribers threshold value to *600* seconds (10 minutes):

```
threshold poll total-subscriber interval 600
```

threshold poll aaa-acct-archive-queue-size

Configures the polling interval over which to measure AAA accounting archive message queue size.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold poll aaa-acct-archive-queue-size1 interval *duration*

default threshold poll aaa-acct-archive-queue-size1 interval

threshold poll aaa-acct-archive-queue-size2 interval *duration*

default threshold poll aaa-acct-archive-queue-size2 interval

threshold poll aaa-acct-archive-queue-size3 interval *duration*

default threshold poll aaa-acct-archive-queue-size3 interval

default

Restores the specified parameter to its default value 900 seconds.

interval *duration*

Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for the AAA accounting archive queue size threshold:

```
threshold poll aaa-acct-archive-queue-size1 interval 600
```

threshold poll aaa-acct-archive-size

Configures the polling interval over which to count archived AAA accounting messages.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold poll aaa-acct-archive-size interval *duration*

default threshold poll aaa-acct-archive-size interval

default

Restores the specified parameter to its default value 300 seconds.

interval *duration*

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for the AAA accounting archive size threshold:

```
threshold poll aaa-acct-archive-size interval 600
```

threshold poll aaa-acct-failure

Configures the polling interval over which to count failed AAA accounting requests.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold poll aaa-acct-failure interval *duration*

default threshold poll aaa-acct-failure interval

default

Restores the specified parameter to its default value 300 seconds.

interval *duration*

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for the AAA accounting failure threshold:

```
threshold poll aaa-acct-failure interval 600
```

threshold poll aaa-acct-failure-rate

Configures the polling interval over which to measure the percentage of AAA accounting failures.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold poll aaa-acct-failure-rate interval *duration*

default threshold poll aaa-acct-failure-rate interval

default

Restores the specified parameter to its default value 300 seconds.

interval *duration*

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for the AAA accounting failure rate threshold:

```
threshold poll aaa-acct-failure-rate interval 600
```

threshold poll aaa-auth-failure

Configures the polling interval over which to count failed authentication requests.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold poll aaa-auth-failure interval *duration*

default threshold poll aaa-auth-failure interval

default

Restores the specified parameter to its default value 300 seconds.

interval *duration*

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for the AAA authentication failure threshold:

```
threshold poll aaa-auth-failure interval 600
```

threshold poll aaa-auth-failure-rate

Configures the polling interval over which to measure the percentage of AAA authentication failures.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold poll aaa-auth-failure-rate interval *duration*

default threshold poll aaa-auth-failure-rate interval

default

Restores the specified parameter to its default value 300 seconds.

interval *duration*

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for the AAA authentication failure rate threshold:

```
threshold poll aaa-auth-failure-rate interval 600
```

threshold poll aaa-retry-rate

Configures the polling interval over which to measure the percent of AAA request message retries.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold poll aaa-retry-rate interval *duration*

default threshold poll aaa-retry-rate interval

default

Restores the specified parameter to its default value 300 seconds.

interval *duration*

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for the AAA retry rate threshold:

```
threshold poll aaa-retry-rate interval 600
```

threshold poll aaamgr-request-queue

Configures the polling interval over which to count the number of AAA Manager Requests for each AAA manager process.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold poll aaamgr-request-queue interval *duration*

default threshold poll aaamgr-request-queue interval

default

Restores the specified parameter to its default value 300 seconds.

interval *duration*

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for the AAA manager request queue threshold:

```
threshold poll aaamgr-request-queue interval 600
```

threshold poll asngw-auth-failure

Configures the polling interval over which to count or measure the thresholding value for ASN Gateway authentication failure.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

threshold poll asngw-auth-failure interval *dur*

default threshold poll asngw-auth-failure interval

default

Restores the specified parameter to its default value 300 seconds.

interval *dur*

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for the ASN Gateway authentication failure threshold:

```
threshold poll asngw-auth-failure interval 600
```

threshold poll asngw-handoff-denial

Configures the polling interval over which to count or measure the thresholding value for ASN Gateway hand-off denial.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

threshold poll asngw-handoff-denial interval *dur*

default threshold poll asngw-handoff-denial interval

default

Restores the specified parameter to its default value 300 seconds.

interval *dur*

Default: 300 seconds.
Specifies the polling interval time in seconds.
dur is an integer from 30 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for hand-off denial threshold:

```
threshold poll asngw-handoff-denial interval 600
```

threshold poll asngw-max-eap-retry

Configures the polling interval over which to count or measure the thresholding value for maximum Extensible Authentication Protocol (EAP) authentication retries.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

threshold poll asngw-max-eap-retry interval *dur*

default threshold poll asngw-max-eap-retry interval

default

Restores the specified parameter to its default value 300 seconds.

interval *dur*

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for maximum EAP authentication retry threshold:

```
threshold poll asngw-max-eap-retry interval 600
```

threshold poll asngw-network-entry-denial

Configures the polling interval over which to count or measure the thresholding value for network entry denial to an MS.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

threshold poll asngw-network-entry-denial interval *dur*

default threshold poll asngw-network-entry-denial interval

default

Restores the specified parameter to its default value 300 seconds.

interval *dur*

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for network entry denial threshold:

```
threshold poll asngw-network-entry-denial interval 600
```

threshold poll asngw-r6-invalid-nai

Configures the polling interval over which to count or measure the thresholding value for invalid Network Access Identifiers (NAIs) in R6 messages.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

threshold poll asngw-r6-invalid-nai interval *dur*

default threshold poll asngw-r6-invalid-nai interval

default

Restores the specified parameter to its default value 300 seconds.

interval *dur*

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for invalid NAIs in R6 messages threshold:

```
threshold poll asngw-r6-invalid-nai interval 600
```

threshold poll asngw-session-setup-timeout

Configures the polling interval over which to count or measure the thresholding value for session setup timeout.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

threshold poll asngw-session-setup-timeout interval *dur*

default threshold poll asngw-session-setup-timeout interval

default

Restores the specified parameter to its default value 300 seconds.

interval *dur*

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for session setup timeout threshold:

```
threshold poll asngw-session-setup-timeout interval 600
```

threshold poll asngw-session-timeout

Configures the polling interval over which to count or measure the thresholding value for session timeout.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

threshold poll asngw-session-timeout interval *dur*

default threshold poll asngw-session-timeout interval

default

Restores the specified parameter to its default value (300 seconds).

interval *dur*

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for session timeout threshold:

```
threshold poll asngw-session-timeout interval 600
```

threshold poll cdr-file-space

This command configures the polling interval for Charging Data Record (CDR) File Space Usage threshold.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

threshold poll cdr-file-space interval *duration*

default threshold poll cdr-file-space interval

default

Uses the default polling interval.
Default: 300 seconds

interval *duration*

Specifies the polling interval (in seconds) for the CDR File Space Usage threshold.
duration must be an integer from 60 through 60000.

Usage

This command configures the polling interval for CDR File Space Usage threshold.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for the CDR file space usage threshold:

```
threshold poll cdr-file-space interval 600
```

threshold poll contfilt-block

This command configures the polling interval Content Filtering Block threshold.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

threshold poll contfilt-block interval *duration*

default threshold poll contfilt-block interval

default

Uses the default threshold polling interval.
Default: 300 seconds

interval *duration*

Specifies the polling interval (in seconds) for the Content Filtering Block threshold.
duration must be an integer from 60 through 60000.

Usage

This command configures the polling interval Content Filtering Block threshold.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for the content filtering blocking threshold:

```
threshold poll contfilt-block interval 600
```

threshold poll contfilt-rating

This command configures the polling interval for the Content Filtering Rating threshold.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

threshold poll contfilt-rating interval *duration*

default threshold poll contfilt-rating interval

default

Uses the default threshold polling interval.
Default: 300 seconds

interval *dur*

Specifies the polling interval (in seconds) for the Content Filtering Rating threshold.
duration must be an integer from 60 through 60000.

Usage

This command configures the polling interval for the Content Filtering Rating threshold.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for the content filtering rating processing threshold:

```
threshold poll contfilt-rating interval 600
```

threshold poll dcca-bad-answers

This command configures the polling interval for DCCA Bad Answers threshold—invalid or bad response to the system from the Diameter server.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

threshold poll dcca-bad-answers interval *duration*

default threshold poll dcca-bad-answers interval

default

Uses the default threshold polling interval.
Default: 900 seconds

interval *duration*

Specifies the polling interval (in seconds) for the DCCA Bad Answers threshold.
duration must be an integer from 60 through 60000.

Usage

This command configures the poling interval for DCCA Bad Answers threshold.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholding in this chapter.

Example

The following command configures the polling interval to *600* seconds for invalid or bad response threshold to the system from Diameter server:

```
threshold poll dcca-rating-failed interval 600
```

threshold poll dcca-protocol-error

This command configures the polling interval for Diameter Credit-Control Application (DCCA) Protocol Error threshold.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

threshold poll dcca-protocol-error interval *duration*

default threshold poll dcca-protocol-error interval

default

Uses the default threshold polling interval.
Default: 900 seconds

interval *duration*

Specifies the polling interval (in seconds) for the DCCA Protocol Error threshold.
duration must be an integer from 60 through 60000.

Usage

Use this the polling interval for DCCA Protocol Error threshold.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholding in this chapter.

Example

The following command configures the polling interval to *600* seconds for the DCCA protocol error threshold:

```
threshold poll dcca-protocol-error interval 600
```

threshold poll dcca-rating-failed

This command configures the polling interval for Diameter Credit-Control Application (DCCA) Rating Failed threshold.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

threshold poll dcca-rating-failed interval *duration*

default threshold poll dcca-rating-failed interval

default

Uses the default polling interval.
Default: 900 seconds

interval *duration*

Specifies the polling interval (in seconds) for the DCCA Rating Failed threshold.
duration must be an integer from 60 through 60000.

Usage

This command configures the polling interval for DCCA Rating Failed threshold.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholding in this chapter.

Example

The following command configures the polling interval to *600* seconds for the Diameter Credit Control Application (DCCA) Rating Group (content-id) request reject thresholds:

```
threshold poll dcca-rating-failed interval 600
```

threshold poll dcca-unknown-rating-group

This command configures the polling interval for Diameter Credit-Control Application (DCCA) Unknown Rating Group threshold.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

threshold poll dcca-unknown-rating-group interval *duration*

default threshold poll dcca-unknown-rating-group interval

default

Uses the default polling interval.
Default: 900 seconds

interval *duration*

Specifies the polling interval (in seconds) for the DCCA Unknown Rating Group threshold.
duration must be an integer from 60 through 60000.

Usage

This command configures the polling interval for DCCA Unknown Rating Group threshold.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholding in this chapter.

Example

The following command configures the polling interval to *600* seconds to threshold for the unknown DCCA Rating Group (content-id) returned by Diameter to system:

```
threshold poll dcca-unknown-rating-group interval 600
```

threshold poll diameter-retry-rate

This command configures the polling interval for the Diameter Credit-Control Application (DCCA) Diameter Retry Rate threshold.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

threshold poll diameter-retry-rate interval *duration*

default threshold poll diameter-retry-rate interval

default

Uses the default polling interval.
Default: 300 seconds

interval *duration*

Specifies the polling interval (in seconds) for the Diameter Retry Rate threshold.
duration must be an integer from 60 through 60000. The input will be rounded up to the closest multiple of 30.

Usage

This command specifies the polling interval for Diameter Retry Rate threshold.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands in this chapter for additional information on the system's support for thresholding.

Example

The following command configures the Diameter Retry Rate threshold polling interval to *600* seconds:

```
threshold poll diameter-retry-rate interval 600
```

threshold poll edr-file-space

This command configures the polling interval for Event Data Record (EDR) File Space Usage threshold.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

threshold poll edr-file-space interval *duration*

interval *duration*

Default: 300 seconds.
Specifies the polling interval (in seconds) for the EDR File Space Usage threshold.
duration must be an integer from 60 through 60000.

Usage

This command configures the polling interval for EDR File Space Usage threshold

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring ecs** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval to *600* seconds for the EDR file space usage threshold:

```
threshold poll edr-file-space interval 600
```

threshold poll mme-attach-failure

This command configures the polling interval to count the MME Attach Failure messages across all MME services in the system.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

threshold poll mme-attach-failure interval *dur*

default threshold poll mme-attach-failure interval

default

Restores the polling interval value to its default value of 900 seconds.

interval *dur*

Default: 900 seconds.
Specifies the polling interval (in seconds) for counting MME Attach Failure messages across all MME services in the system.
dur must be an integer from 30 through 60000 in multiples of 30.

Usage

Use this command to configure the polling interval to count the MME Attach Failure messages across all MME services in the system to generate threshold value.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring mme-service** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval of *600* seconds to count the MME Attach Failure messages for threshold limit:

```
threshold poll mme-attach-failure interval 600
```

threshold poll mme-auth-failure

This command configures the polling interval to count the MME Authentication Failure messages across all MME services in the system.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

threshold poll mme-auth-failure interval *dur*

default threshold poll mme-auth-failure interval

default

Restores the specified poll interval value to its default value of 900 seconds.

interval *dur*

Default: 900 seconds.
Specifies the polling interval (in seconds) for counting MME Authentication Failure messages across all MME services in the system.
dur must be an integer from 30 through 60000 in multiples of 30.

Usage

Use this command to configure the polling interval to count the MME Auth Failure messages across all MME services in the system to generate threshold value.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring mme-service** and other threshold commands for additional information on the system's support for thresholds in this chapter.

Example

The following command configures the polling interval of *600* seconds to count the MME Auth Failure messages for threshold limit:

```
threshold poll mme-auth-failure interval 600
```

threshold poll total-hnbgw-hnb-sessions

This command configures the polling interval over which to count or measure the thresholding value for the total number of IuH sessions between the HNB and HNB-GW to count across all the HNB-GW services on a system to trigger an alert or alarm.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

threshold poll total-hnbgw-hnb-sessions interval *time*

default threshold poll total-hnbgw-hnb-sessions interval

default

Restores the threshold polling interval value to its default value of 900 seconds.

interval *time*

Default: 900 seconds
Specifies the polling interval (in seconds) for counting the total number of IuH sessions between the HNB and HNB-GW across all the HNB-GW services on a system.
time must be an integer from 30 through 60000.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.

Important: To enable SNMP trap for threshold monitoring of this threshold use **snmp trap enable ThreshTotalHNBGWHnbSess** command in this mode.

Example

The following command configures the polling interval for counting the total number of IuH sessions between HNB and HNB-GW across all the HNB-GW services on a system, to *600* seconds (10 minutes):

```
threshold poll total-hnbgw-hnb-sessions interval 600
```

threshold poll total-hnbgw-iu-sessions

This command configures the polling interval over which to count or measure the thresholding value for the total number of subscriber sessions on HNB-GW service (over Iu-CS/Iu-PS interface) to count across all the HNB-GW services on a system to trigger alert or alarm.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

threshold poll total-hnbgw-iu-sessions interval *time*

default threshold poll total-hnbgw-iu-sessions interval

default

Restores the threshold poll interval value to its default value of 900 seconds.

interval *time*

Default: 900 seconds
Specifies the polling interval (in seconds) for counting the total number of subscriber sessions across all the HNB-GW services on a system.
time must be an value from 30 through 60000.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.

Important: To enable SNMP trap for threshold monitoring to this threshold use **snmp trap enable ThreshTotalHNBGWIuSess** command in this mode.

Example

The following command configures the polling interval for counting the total number of subscriber sessions across all the HNB-GW services on a system, to *600* seconds (10 minutes):

```
threshold poll total-hnbgw-iu-sessions interval 600
```

threshold poll total-hnbgw-ue-sessions

This command configures the polling interval over which to count or measure the thresholding value for the total number of UEs connected to HNB-GW service to count across all the HNB-GW services on a system to trigger alert or alarm.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

threshold poll total-hnbgw-iu-sessions interval *time*

default threshold poll total-hnbgw-iu-sessions interval

default

Restores the threshold poll interval value to its default value of 900 seconds.

interval *time*

Default: 900 seconds
Specifies the polling interval (in seconds) for counting the total number UEs connected to an HNB-GW service across all the HNB-GW services on a system.
time must be an integer from 30 through 60000.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.

Important: To enable SNMP trap for threshold monitoring to this threshold use **snmp trap enable ThreshTotalHNBGWUeSess** command in this mode.

Example

The following command configures the polling interval for the total number of UEs connected to an HNB-GW service across all the HNB-GW services on a system, to *600* seconds (10 minutes):

```
threshold poll total-hnbgw-ue-sessions interval 600
```

threshold poll total-mme-sessions

This command configures the polling interval over which to count or measure the thresholding value for MME sessions on the system.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

threshold poll total-mme-sessions interval *time*

default threshold poll total-mme-sessions interval

default

Restores the threshold poll interval value to its default value of 900 seconds.

interval *time*

Default: 900 seconds
Specifies the polling interval (in seconds) for counting the total number of MME sessions on the system. *time* must be an ny integer from 30 through 60000.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.

Example

The following command configures the polling interval for the total MME session threshold polling duration value to *600* seconds (10 minutes):

```
threshold poll total-mme-sessions interval 600
```

threshold poll port-rx-utilization

Enables the generation of alerts or alarms based on the port utilization percentage for data received during the polling interval.

Product

All

Privilege

Administrator Security Administrator

Syntax

threshold poll port-rx-utilization interval *seconds*

interval *seconds*

Configures the threshold polling interval in multiples of 30 seconds. *seconds* is an integer from 30 to 60000

Usage

Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis configured using the port *port-type slot#/port#* command syntax.

Important: This command is not available on all platforms

Important: Ports configured for half-duplex do not differentiate between data received and data transmitted. (The transmitted and received percentages are combined.) Therefore, to avoid redundant alarms, it is recommended that only the receive **or** transmit utilization threshold be configured.

Example

Use the following example to configure a threshold poll interval of *300* seconds (5 minutes)

```
threshold poll port-rx-utilization interval 300
```

threshold poll port-tx-utilization

Enables the generation of alerts or alarms based on the port utilization percentage for data transmitted during the polling interval.

Product

All

Privilege

Administrator Security Administrator

Syntax

threshold poll port-tx-utilization interval *seconds*

interval *seconds*

Configures the threshold polling interval in multiples of 30 seconds. *seconds* is an integer from 30 through 60000

Usage

Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis configured using the port *port-type slot#/port#* command syntax.

Important: This command is not available on all platforms

Important: Ports configured for half-duplex do not differentiate between data received and data transmitted. (The transmitted and received percentages are combined.) Therefore, to avoid redundant alarms, it is recommended that only the receive **or** transmit utilization threshold be configured.

Example

Use the following example to configure a threshold poll interval of *300* seconds (5 minutes)

```
threshold poll port-tx-utilization interval 300
```

threshold poll port-high-activity

Enables the generation of alerts or alarms based on the overall port utilization percentage during the polling interval.

Product

All

Privilege

Administrator Security Administrator

Syntax

threshold poll port-high-activity interval *seconds*

interval *seconds*

Configures the threshold polling interval in multiples of 30 seconds. *seconds* is an integer from 30 through 60000

Usage

High port activity thresholds generate alerts or alarms based on the peak utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis. Alerts or alarms are triggered for high port activity based on the following rules:
Enter condition: Actual percent peak utilization of a port is greater than or equal to the high threshold.
Clear condition: Actual percent peak utilization of a port is less than the low threshold.
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.This threshold is configured on a per-port basis configured using the port *port-type slot#/port#* command syntax.

Important: This command is not available on all platforms

Example

Use the following example to configure the polling interval over which to measure for high port activity to *300* seconds:

```
threshold poll port-high-activity interval 300
```

threshold poll route-service

This command configures the polling interval over which to count or measure the thresholding value for route services on the system.

Product

All

Privilege

Administrator Security Administrator

Syntax

threshold poll route-service interval *dur*

default threshold poll route-service interval

default

Restores the threshold poll interval value to its default value of 900 seconds.

interval *time*

Default: 900 seconds
Specifies the polling interval (in seconds) for counting the total number of BGP routes on the system.
dur is any integer from 30 through 60000.

Usage

This command dictates the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.

Example

The following command configures the polling interval for the total BGP routes threshold polling duration value to *600* seconds (10 minutes):

```
hreshold poll route-service interval 600
```

threshold poll tpo-dns-failure

This command configures the threshold polling interval for monitoring TPO DNS resolution failures.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

threshold poll tpo-dns-failure interval *interval*

default threshold poll tpo-dns-failure interval

default

Configures this command with the default polling interval.
Default: 900 seconds

interval

Specifies the polling interval (in seconds) for monitoring TPO DNS resolution failures.
interval must be an integer from 30 through 60000. The system rounds up the value to the closest multiple of 30.

Usage

Use this command to configure the threshold polling interval for monitoring TPO DNS resolution failures.

Example

The following command configures the polling interval for TPO DNS resolution failures threshold to *600* seconds:

```
threshold poll tpo-dns-failure interval 600
```

threshold poll tpo-low-compression-gain

This command configures the threshold polling interval for monitoring TPO low-compression-gain results.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

threshold poll tpo-low-compression-gain interval *interval*

default threshold poll tpo-low-compression-gain interval

default

Configures this command with the default polling interval.
Default: 900 seconds

interval

Specifies the polling interval (in seconds) for monitoring TPO low-compression-gain results.
interval must be an integer from 30 through 60000. The system rounds up the value to the closest multiple of 30.

Usage

Use this command to configure the threshold polling interval for monitoring TPO low-compression-gain results.

Example

The following command configures the polling interval for TPO low-compression-gain results threshold to *600* seconds:

```
threshold poll tpo-low-compression-gain interval 600
```

threshold poll tpo-rto-timeout

This command configures the threshold polling interval for monitoring TPO retransmission timeouts (RTOs).

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

threshold poll tpo-rto-timeout interval *interval*

default threshold poll tpo-rto-timeout interval

default

Configures this command with the default polling interval.
Default: 900 seconds

interval

Specifies the polling interval (in seconds) for monitoring TPO retransmission timeouts.
interval must be an integer from 30 through 60000. The system rounds up the value to the closest multiple of 30.

Usage

Use this command to configure the threshold polling interval for monitoring TPO retransmission timeouts.

Example

The following command configures the polling interval for TPO retransmission timeouts threshold to *600* seconds:

```
threshold poll tpo-rto-timeout interval 600
```

threshold ppp-setup-fail-rate

Configures point-to-point protocol (PPP) setup failure rate percentage thresholds.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

threshold ppp-setup-fail-rate *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold rate percentage for PPP setup failures experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold rate percentage for PPP setup failures experienced by the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

PPP setup failure rate thresholds generate alerts or alarms based on the rate of call setup failures experienced by the system during the specified polling interval. The failure rate is the percentage of failures as determined by number of PPP setup failures divided by the total number of PPP sessions initiated.
Alerts or alarms are triggered for PPP setup failure rates based on the following rules:

- **Enter condition:** Actual number of call setup failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of call setup failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a PPP setup failure rate high percentage threshold of *50* percent and a clear threshold of *45* percent:

```
threshold ppp-setup-fail-rate 50 clear 45
```

threshold route-service bgp-routes

This command configures the percentage threshold limits for route services to BGP routes.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

threshold route-service bgp-routes *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold rate percentage for BGP routes on the system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold rate percentage for BGP routes on the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to configure a threshold in percentage of maximum BGP routes allowed. If the percentage of the number of BGP routes in a context (including all VRFs) reaches *high_thresh*, a notification is generated. Optionally, if the threshold subsystem is configured in 'alarm' mode, a **Threshold_Clear** notification is generated when the percentage of the number of BGP routes in a context (including all VRFs) goes below *low_thresh*. The maximum number of BGP routes is also sent by BGP task when getting the stats
Alerts or alarms are triggered for BGP routes based on the following rules:

- **Enter condition:** Actual number of call setup failures is greater than the high threshold.
- **Clear condition:** Actual number of call setup failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures system for high threshold of *50* percent and a clear threshold of *45* percent:

```
threshold route-service bgp-routes 50 clear 45
```

threshold rp-setup-fail-rate

Configures RP setup failure rate thresholds.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

threshold rp-setup-fail-rate *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold rate percentage for RP setup failures experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold rate percentage for RP setup failures experienced by the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

RP setup failure rate thresholds generate alerts or alarms based on the rate of call setup failures experienced by the system during the specified polling interval. The failure rate is the percentage of failures as determined by number of Registration Request Messages rejected divided by the total number of Registration Request Messages received.
Alerts or alarms are triggered for RP setup failure rates based on the following rules:

- **Enter condition:** Actual number of call setup failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of call setup failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a RP setup failure rate high threshold of *50* percent and a clear threshold of *45* percent:

```
threshold rp-setup-fail-rate 50 clear 45
```

threshold spc-cpu-memory-usage

This command has been renamed to **`threshold mgmt-cpu-memory-usage`**. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.

Important: This command is not supported on all platforms.

threshold spc-cpu-utilization

This command has been renamed to **`threshold mgmt-cpu-utilization`**. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.

threshold storage-utilization

Configures SMC flash memory utilization thresholds.

Product

All

Privilege

Security Administrator, Administrator

Syntax

threshold storage-utilization *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 90
Specifies the high threshold memory utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

clear *low_thresh*

Default: 90
Specifies the low threshold memory utilization percentage that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Flash memory utilization thresholds generate alerts or alarms based on the utilization percentage of the flash memory on each installed SMC during the specified polling interval. Although, a single threshold is configured for both SMCs, separate alerts or alarms can be generated for each.
Alerts or alarms are triggered for CompactFlash memory utilization based on the following rules:

- **Enter condition:** Actual percentage memory utilization is greater than or equal to the high threshold.
- **Clear condition:** Actual percentage memory utilization is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold flash utilization percentage of *85* for a system using the Alert thresholding model:

```
threshold storage-utilization 85
```

threshold subscriber active

Configures thresholds for active subscribers in the system.

Product

PDSN, GGSN, SGSN, HA

Privilege

Security Administrator, Administrator

Syntax

threshold subscriber active *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of active subscriber sessions facilitated by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of active subscriber sessions facilitated by the system that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Active subscriber thresholds generate alerts or alarms based on the total number of active subscriber sessions facilitated by the system during the specified polling interval.
Alerts or alarms are triggered for active subscriber totals based on the following rules:

- **Enter condition:** Actual total number of active subscriber sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of active subscriber sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures an active subscriber high threshold count of *150000* and a low threshold of *100000* for a system using the Alarm thresholding model:

```
threshold subscriber active 150000 clear 100000
```

threshold subscriber total

Configures total subscriber thresholds for the system.

Product

PDSN, GGSN, HA

Privilege

Security Administrator, Administrator

Syntax

threshold subscriber total *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of subscriber sessions (active and dormant) facilitated by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of subscriber sessions (active and dormant) facilitated by the system that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Total subscriber thresholds generate alerts or alarms based on the total number of subscriber sessions (active and dormant) facilitated by the system during the specified polling interval.
Alerts or alarms are triggered for subscriber totals based on the following rules:

- **Enter condition:** Actual total number of subscriber sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of subscriber sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures an active subscriber high threshold count of *450000* and a low threshold of *250000* for a system using the Alarm thresholding model:

```
threshold subscriber total 450000 clear 250000
```

threshold total-ggsn-sessions

Configures thresholds for the total number of GGSN sessions across all the services in the system.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

threshold total-ggsn-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0 (Disabled)
Specifies the high threshold number of total GGSN sessions across all the sessions in the system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0 (Disabled)
Specifies the low threshold number of total GGSN sessions that maintains a previously generated alarm condition. If the number of GGSN sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of GGSN sessions across all the services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of GGSN sessions based on the following rules:

- **Enter condition:** Actual total number of GGSN sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of GGSN sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total GGSN session high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-ggsn-sessions 10000
```

threshold total-gprs-sessions

Configures thresholds for the total number of GPRS sessions in the system.

Product

SGSN

Privilege

Administrator

Syntax

threshold total-gprs-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of total GPRS sessions for all GPRS services that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 1 through 2000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of total GPRS sessions for all GPRS services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 2000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of GPRS sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for GPRS sessions based on the following rules:

- **Enter condition:** Actual total number of GPRS sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of GPRS sessions is less than the low threshol.d

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of GPRS sessions high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-gprs-sessions 10000
```

threshold total-gprs-pdp-sessions

Configures thresholds for the total number of PDP contexts per GPRS sessions in the system.

Product

SGSN

Privilege

Administrator

Syntax

threshold total-gprs-pdp-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of total PDP contexts per GPRS session for all GPRS services that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 1 through 2000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of total PDP contexts per GPRS session for all GPRS services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 2000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of GPRS sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for GPRS sessions based on the following rules:

- **Enter condition:** Actual total number of PDP Contexts is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of PDP contexts is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of PDP contexts per GPRS session high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-gprs-pdp-sessions 10000
```

threshold total-ha-sessions

Configures thresholds for the total number of HA sessions across all services in the system.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

threshold total-ha-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of HA sessions for all HA services that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of HA sessions for all HA services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of HA sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for HA sessions based on the following rules:

- **Enter condition:** Actual total number of HA sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of HA sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of HA sessions high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-ha-sessions 10000
```

threshold total-hnbgw-hnb-sessions

Use this command to configure alarm or alert thresholds for the total number of IuH sessions between HNB and HNB-GW across all the HNB-GW services in the system.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

threshold total-hnbgw-hnb-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0 (Disabled)
Specifies the high threshold for the total number of HNB-HNB-GW sessions on IuH interfaces across all HNB-GW services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0 (Disabled)
Specifies the low threshold for the total number of HNB-HNB-GW sessions on IuH interfaces across all services on a system that maintains a previously generated alarm condition. If the number of HNB-HNB-GW sessions in a system falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to monitor and set alarms or alerts when the total number of HNB-HNB-GW sessions on IuH interface across all HNB-GW services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of HNB-HNB-GW sessions on IuH interface based on the following rules:

- **Enter condition:** Actual total number of HNB-HNB-GW sessions on IuH interface is greater than the high threshold.
- **Clear condition:** Actual total number of HNB-HNB-GW sessions on IuH interfaces is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll total-hnbgw-hnb-sessions** command to configure the polling interval and the **threshold monitoring hnbgw-service** command to enable thresholding for this value.

Important: To enable SNMP trap for threshold monitoring to this threshold use **`snmp trap enable ThreshTotalHNBGWHnbSess`** command in this mode.

Example

The following command configures the total number of HNB-GW-HNB sessions on IuH interfaces to a high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-hnbgw-hnb-sessions 10000
```

threshold total-hnbgw-iu-sessions

Use this command to configure alert or alarm thresholds for the total number of subscriber sessions towards the Core Networks (CN) across all HNB-GW services over Iu interfaces (Iu-CS/Iu-PS interface) on a system.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

threshold total-hnbgw-iu-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0 (Disabled)
Specifies the high threshold for the total number of subscriber sessions towards CN across all HNB-GW services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 3000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0 (Disabled)
Specifies the low threshold for the total number of subscriber sessions towards CN across all services on a system that maintains a previously generated alarm condition. If the number of subscriber sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 3000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to monitor and set alarms or alerts when the total number of subscriber sessions towards CN across all HNB-GW services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of subscriber sessions towards CN across all HNB-GW service on a system based on the following rules:

- **Enter condition:** Actual total number of subscriber sessions across all HNB-GW service on a system is greater than the high threshold.
- **Clear condition:** Actual total number of subscriber sessions across all HNB-GW service on a system is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll total-hnbgw-iu-sessions** command to configure the polling interval and the **threshold monitoring hnbgw-service** command to enable thresholding for this value.

Important: To enable SNMP trap for threshold monitoring to this threshold use **snmp trap enable ThreshTotalHNBGWIuSess** command in this mode.

Example

The following command configures the total number of subscriber sessions towards CN across all HNB-GW services to a high threshold count of *30000* for a system using the Alert thresholding model:

```
threshold total-hnbgw-iu-sessions 30000
```

threshold total-hnbgw-ue-sessions

Use this command to configure alert or alarm thresholds for the total number of UEs connected to an HNB-GW service across all the HNB-GW services in the system.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

threshold total-hnbgw-ue-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0 (Disabled)
Specifies the high threshold for the total number of UEs connected across all HNB-GW services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0 (Disabled)
Specifies the low threshold for the total number of UEs connected to HNB-GW service across all HNB-GW services that maintains a previously generated alarm condition. If the number of UE sessions across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to monitor and set alarms or alerts when the total number of UEs connected to HNB-GW service across all HNB-GW services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of UEs connected across all HNB-GW service on a system based on the following rules:

- **Enter condition:** Actual total number of UEs connected to HNB-GW service across all HNB-GW services on a system is greater than the high threshold.
- **Clear condition:** Actual total number of UEs connected to HNB-GW service across all HNB-GW services on a system is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll total-hnbgw-ue-sessions** command to configure the polling interval and the **threshold monitoring hnbgw-service** command to enable thresholding for this value.

Important: To enable SNMP trap for threshold monitoring to this threshold use **`snmp trap enable ThreshTotalHNBGWUeSess`** command in this mode.

Example

The following command configures the total number of UEs connected to HNB-GW service across all HNB-GW services to a high threshold count of *40000* for a system using the Alert thresholding model:

```
threshold total-hnbgw-ue-sessions 40000
```

threshold total-hsgw-sessions

Configures thresholds for the total number of HSGW sessions across all services in the system.

Product

HSGW

Privilege

Administrator

Syntax

threshold total-hsgw-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold for the number of HSGW sessions for all HSGW services that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 1 through 1500000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold for the number of HSGW sessions for all HSGW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 1500000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of HSGW sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for HSGW sessions based on the following rules:

- **Enter condition:** Actual total number of HSGW sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of HSGW sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of HSGW sessions high threshold count of *500000* for a system using the Alert thresholding model:

```
threshold total-hsgw-sessions 500000
```

threshold total-lma-sessions

Configures thresholds for the total number of Local Mobility Anchor (LMA) sessions across all services in the system.

Product

P-GW

Privilege

Administrator

Syntax

threshold total-lma-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of LMA sessions for all LMA services that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 1 through 1500000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of LMA sessions for all LMA services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 1500000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of LMA sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for LMA sessions based on the following rules:

- **Enter condition:** Actual total number of LMA sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of LMA sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of LMA sessions high threshold count of *500000* for a system using the Alert thresholding model:

```
threshold total-lma-sessions 500000
```

threshold total-lns-sessions

Configures thresholds for the total number of L2TP Network Server (LNS) sessions in the system.

Product

PDSN, GGSN, HA

Privilege

Security Administrator, Administrator

Syntax

threshold total-lns-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of total LNS sessions that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer value from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of total LNS sessions that maintains a previously generated alarm condition. If the number of LNS sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of LNS sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of LNS sessions based on the following rules:

- **Enter condition:** Actual total number of LNS sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of LNS sessions is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total LNS session high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-lns-sessions 10000
```

threshold total-mme-sessions

Use this command to configure thresholds for the total number of MME sessions across all the MME services in the system.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

threshold total-mme-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0 (Disabled)
Specifies the high threshold number of total MME sessions that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer value from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0 (Disabled)
Specifies the low threshold number of total MME sessions that maintains a previously generated alarm condition. If the number of MME sessions, across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to monitor and set alarms or alerts when the total number of MME sessions across all the MME services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of MME sessions based on the following rules:

- **Enter condition:** Actual total number of MME sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of MME sessions is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll total-mme-sessions** command to configure the polling interval and the **threshold monitoring mme-service** command to enable thresholding for this value.

Example

The following command configures a total MME session high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-mme-sessions 10000
```

threshold total-pdsn-sessions

Configures thresholds for the total number of PDSN sessions in the system.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

threshold total-pdsn-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of total PDSN sessions that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of total PDSN sessions that maintains a previously generated alarm condition. If the number of PDSN sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of PDSN sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of PDSN sessions based on the following rules:

- **Enter condition:** Actual total number of PDSN sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of PDSN sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total PDSN session high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-pdsn-sessions 10000
```

threshold total-pgw-sessions

Configures thresholds for the total number of P-GW sessions across all services in the system.

Product

P-GW

Privilege

Administrator

Syntax

threshold total-pgw-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of P-GW sessions for all P-GW services that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 1 through 1500000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of P-GW sessions for all P-GW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 1500000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of P-GW sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for P-GW sessions based on the following rules:

- **Enter condition:** Actual total number of P-GW sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of P-GW sessions is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of P-GW sessions high threshold count of *500000* for a system using the Alert thresholding model:

```
threshold total-pgw-sessions 500000
```

threshold total-sgw-sessions

Configures thresholds for the total number of S-GW sessions across all services in the system.

Product

S-GW

Privilege

Administrator

Syntax

threshold total-sgw-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of S-GW sessions for all S-GW services that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 1 through 1500000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of S-GW sessions for all S-GW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 1500000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of S-GW sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for S-GW sessions based on the following rules:

- **Enter condition:** Actual total number of S-GW sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of S-GW sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of S-GW sessions high threshold count of *500000* for a system using the Alert thresholding model:

```
threshold total-sgw-sessions 500000
```

threshold total-sgsn-sessions

Configures thresholds for the total number of SGSN sessions in the system.

Product

SGSN

Privilege

Administrator

Syntax

threshold total-sgsn-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of total SGSN sessions for all SGSN services that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 1 through 2000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of total SGSN sessions for all SGSN services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 2000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of SGSN sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for SGSN sessions based on the following rules:

- **Enter condition:** Actual total number of SGSN sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of SGSN sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of SGSN sessions high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-sgsn-sessions 10000
```

threshold total-sgsn-pdp-sessions

Configures thresholds for the total number of PDP contexts per SGSN sessions in the system.

Product

SGSN

Privilege

Administrator

Syntax

threshold total-sgsn-pdp-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0
Specifies the high threshold number of total PDP contexts per SGSN session for all SGSN services that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 1 through 2000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0
Specifies the low threshold number of total PDP contexts per SGSN session for all SGSN services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 2000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of SGSN sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for SGSN sessions based on the following rules:

- **Enter condition:** Actual total number of PDP contexts is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of PDP contexts is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of PDP contexts per SGSN session high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-sgsn-pdp-sessions 10000
```

threshold tpo-dns-failure

This command configures thresholds for monitoring TPO DNS resolution failures.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

threshold tpo-dns-failure *high_thresh* **[clear** *low_thresh* **]**

default threshold tpo-dns-failure

default

Configures this command with the default threshold setting.
Default: 0—disabled

high_thresh

Specifies that if in a polling interval the number of TPO DNS failures experienced by the system meets or exceeds *high_thresh* an alert or alarm should be generated.
high_thresh is an integer from 0 through 300000.
Default: 0

clear *low_thresh*

Specifies that if, within the polling interval, the number of TPO DNS failures experienced by the system falls below *low_thresh* a clear alarm should be generated.
low_thresh is an integer from 0 through 300000.
Default: 0

Usage

Use this command to configure thresholds for monitoring TPO DNS resolution failures.

threshold tpo-low-compression-gain

This command configures thresholds for monitoring TPO low-compression-gain comparison results.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

threshold tpo-low-compression-gain *high_thresh* **[clear** *low_thresh* **]**

default threshold tpo-low-compression-gain

default

Configures this command with the default threshold setting.
Default: 0—disabled

high_thresh

Specifies that if in a polling interval the number of TPO low-compression-gain comparison results experienced by the system meets or exceeds *high_thresh* an alert or alarm is generated.
high_thresh is an integer from 0 through 300000.
Default: 0

clear *low_thresh*

Specifies that if, within the polling interval, the number of TPO low-compression-gain comparison results experienced by the system falls below *low_thresh* a clear alarm is generated.
low_thresh is an integer from 0 through 300000.
Default: 0

Usage

Use this command to configure thresholds for monitoring TPO DNS resolution failures.

threshold tpo-rto-timeout

This command configures thresholds for monitoring TPO retransmission timeouts (RTOs).

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

threshold tpo-rto-timeout *high_thresh* **[clear** *low_thresh* **]**

default threshold tpo-rto-timeout

default

Configures this command with the default threshold setting.
Default: 0—disabled

high_thresh

Specifies that if in a polling interval the number of TPO RTOs experienced by the system meets or exceeds *high_thresh* an alert or alarm should be generated.
high_thresh is an integer from 0 through 300000.
Default: 0

clear *low_thresh*

Specifies that if, within the polling interval, the number of TPO RTOs experienced by the system falls below *low_thresh* a clear alarm should be generated.
low_thresh is an integer from 0 through 300000.
Default: 0

Usage

Use this command to configure thresholds for monitoring TPO DNS resolution failures.

timestamps

Enables/disables the generation of a timestamp in response to each commands entered. The timestamp does not appear in any logs as it is a CLI output only. This command affects all future CLI sessions. Use the **timestamps** command in the Exec Mode to change the behavior for the current CLI session only.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
timestamps

no timestamps
```

no

Disables generation of timestamps for each command entered. When omitted, the output of a timestamp for each entered command is enabled.

Usage

Enable the timestamps when logging a CLI session on a remote terminal such that each command will have a line of text indicating the time when the command was entered.

Example

```
timestamps

no timestamps
```

upgrade limit

Configures upgrade session limits that trigger when the system may execute the software upgrade.

Product

All

Privilege

Security Administrator, Administrator

Syntax

upgrade limit [time *session_life* **] [usage** *session_num* **]**

upgrade limit

This command issued with no keywords sets all parameters to their defaults.

time *session_life*

Default: 120
Defines the maximum number of minutes that a session may exist on the system undergoing a software upgrade, before it is terminated by the system. As individual user sessions reach this lifetime limit, the system terminates the individual session(s). *session_life* must be an integer ranging from 1 through 1440.

usage *session_num*

Default: 100
This keyword defines a low threshold limit of sessions running either on a packet processing card or system-wide. When a software upgrade is invoked, this parameter applies to the entire system.
When the threshold is crossed (when the number of sessions on the packet processing card or system is less than this value), the remaining sessions on the card or system are terminated allowing the upgrade to begin. The remaining sessions on the packet processing card or system are terminated regardless of their session life.
session_num must be an integer from 0 through 6000.

Usage

Use this command to configure upgrade session limits that trigger the system to begin executing the software upgrade.

Important: This command is not supported on all platforms.

Important: Software Patch Upgrades are not supported in this release.

Example

The following command sets the number of minutes a session can exist to *200*, and the minimum number of sessions that may exist before terminating them to *50*:

```
upgrade limit time 200 usage 50
```

url-blacklisting database

This command configures URL Blacklisting database directory parameters.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

```
url-blacklisting database { directory path path | max-versions max_versions | override
file file_name }

default url-blacklisting database { directory path | max-versions | override file }
```

default

Configures this command with the default settings.

directory path *path*

Specifies the path to the directory to be used for storing URL Blacklisting databases.
path must be an alphanumeric string of 1 through 255 characters.
Default: /flash/bl

max-versions *max_versions*

Specifies the maximum number of URL Blacklisting database versions to be maintained in the URL Blacklisting database directory path with the base file name specified by the URL Blacklisting database override file.
max_versions must be an integer from 0 through 3.
Default: 0

override file *file_name*

Specifies the URL Blacklisting database override file name.
file_name must be in *name.extension* format. For example, *abc.bin*. And, must be an alphanumeric string of 1 through 10 characters.
Default: optblk.bin

Usage

Use this command to configure URL Blacklisting database directory parameters.

Example

The following command configures the maximum number of URL Blacklisting database versions to be maintained to *3*:

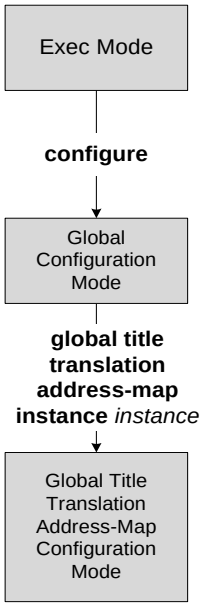
```
url-blacklisting database max-versions 3
```

Chapter 128
Global Title Translation Address-Map Configuration Mode Commands

The Global Title Translation (GTT) Address-Map configuration mode provides the commands to create, configure, and manage a specific GTT address map database.

Upon accessing this mode, your prompt should look similar to the following:

```
[local] <hostname> (config-gtt-assoc-<instance#>)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

associate

This command associates (links) the global title translation (GTT) address-map with a specific GTT association, which includes the translation action rules.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

associate gtt-association *assoc_num* **action id** *id*

no association

no

Removes the association definition from the GTT address-map configuration.

gtt-association *assoc_num*

Identifies a specific GTT association to link (associate) with the GTT address-map.
assoc_num: Must be an integer from 1 to 16.

action id *id*

Identifies a specific action defined in the GTT association database configuration.
id: Must be an integer from 1 to 8.

Usage

Create an association between a specific translation action rule in a specific GTT association and this GTT address-map.

Example

```
associate gtt-association 1 action id 1
```

description

This command defines a descriptive string to facilitate identification of this particular global title translation (GTT) address-map. This is used for operator reference only.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

description *string*

no description

no

Removes the description string from the current global title translation address-map configuration.

string

Specifies the alphanumeric string that is stored. must be from 1 through 127 alphanumeric characters. Strings with spaces must be enclosed in double-quotes. See the example below.

Usage

Use this command to set a description for reference by operators.

Example

description *"GTT for Finnish national carrier."*

end

Exits the configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

exit

Exits the configuration mode and returns to the Global configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Return to the Global configuration mode.

gt-address

Configures the SCCP global title address.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gt-address *gt_address*

no gt-address

no

Removes the GT address from the GTT address-map configuration.

gt_address

Up to 15 digits.

Usage

Define the SCCP short address.

Example

gt-address *01040552873424*

mode

Configures the mode of operation of the SCCP entities.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
mode [ dominant | loadshare ]
```

dominant

This instructs the system to maintain the associated entity as the primary traffic pipe.

loadshare

This instructs the system to distribute the traffic load.

Usage

This command configure load balance for the system.

Example

```
mode loadshare
```

out-address

Identifies the out-going address of the SCCP entity. After this command is completed, the system enters the Out-Address configuration mode. Refer to the Out-Address Configuration Mode chapter for information about commands to define the out-address.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

out-address *name*

no out-address

no

Removes the **out-address** definition from the GSS address-map configuration.

name

Defines a unique string to identify the out-going address using 1 to 63 alphanumeric characters.

Usage

Use this command to identify the address of the SCCP in the GTT configuration. This command also provides access to the Out-Address configuration mode so that the parameters for the out-going SCCP can be configured and maintained.

Example

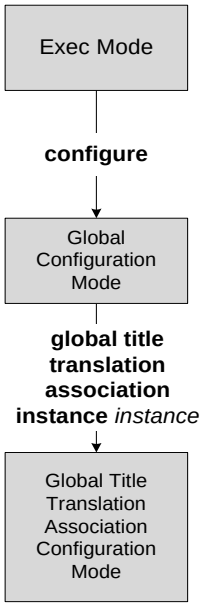
out-address *SCCP_London*

Chapter 129
Global Title Translation Association Configuration Mode Commands

The Global Title Translation (GTT) Association configuration mode provides the commands to create the rules for translating the global titles (destination point codes and subsystem address in the messages) used for routing at the SCCP layer.

Upon accessing this mode, your prompt should look similar to the following:

```
[local] <hostname> (config-gtt-addrmap-<instance#>)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

action

This command configures the actions that determine the operation of rules of the global title translation (GTT).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

action id *id* **type** *action_type* **start-digit** *value* **end-digit** *value*

no action id *id*

id

id uniquely identifies an action. The id must be an integer from 1 to 15.

type *action_type*

The following defines the action rules that will determine how global titles (GT) are translated to locally understood addresses - in most cases point codes (PC). The command can be re-issued multiple times to define multiple action rules.

- **constant:** Defines the starting digit in the range of digits in the incoming global titles that are translated to fixed addresses.
- **fixed:** Defines the starting digit in a fixed range of digits used for performing GTT.
- **gt-to-pc:** Use these digits as first of range of global title digits in incoming message to convert to point code for routing.
- insert-pc: Defines the rule for inserting destination point code before the incoming GTAI and change TT, ES and NAI. Use digits of incoming message global title digits as pc for routing.
- **selins**: Selective insertion type to perform GTT.
- **strip-pc:** Strip first 6 digits from GTAI if first 6 dgts in stripped point code are in INT format.
- **var-asc**: Use a varaible number of digits, in ascending order, to perform GTT.
- **var-des:** Use a variable number of digits. in descending order. to perform GTT.

start-digit *value*

value must be an integer from 0 to 255.

end-digit *value*

value must be an integer from 0 to 255.

Usage

Use this command to create GTT association rules. Rules can be based on ranges of digits or modified ranges depending upon the action types included in the commands.

Example

Use the following command to create a global title translation rule that bases the translation on a fixed range of digits starting at 23 and ending at 122:

```
action id 1 type fixed start-digit 23 end-digit 122
```

description

This command defines a descriptive string to facilitate identification of this particular global title translation (GTT) association. This is used for operator reference only.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

description *string*

no description

string

Specifies the alphanumeric string that is stored. must be from 1 through 127 alphanumeric characters. Strings with spaces must be enclosed in double-quotes. See the example below.

no

Removes the description string from the current global title translation association configuration.

Usage

Use this command to set a description for reference by operators.

Example

The following command sets the description to identify a routing domain for messages transmitted within a national boundary.

```
description "GTT database 2"
```

end

Exits the configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

exit

Exits the configuration mode and returns to the Global configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Return to the Global configuration mode.

gt-format

This command creates an instance of a global title formatting that is applied to the database in the process of address translation. Once the command is completed, the system enters global title (GT) format database configuration mode. The commands for configuration can be found in the GT Format Configuration Mode chapter in this reference guide.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gt-format *format_num*

format_num

- 1: Selects GT-format 1 options which include **nature-of-address** and **odd/even.** Once selected, the system enters GT-Format1 configuration mode.
- 2: Selects GT-format2 options which include **translation-type**. Once selected, the system enters GT-Format2 configuration mode.
- 3: Selects GT-format3 options which include **encoding-scheme**, **numbering-plan,** and **translation-type**. Once selected, the system enters GT-Format3 configuration mode.
- 4: Selects GT-format4 options which include **encoding-scheme**, **nature-of-address, numbering-plan,** and **translation-type**. Once selected, the system enters GT-Format4 configuration mode.

Usage

Selects GT format #2 for the database GTT process.

Example

Use this command to associate the GT format for GTT:

```
gt-format 2
```

variant

This command configures the choice of national standard protocols to associate with the GTT process databases.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

variant *type*

default

Sets the **variant** configuration to **itu**.

type

The following network variant national standards-based protocols are possible:

- **ansi**
- **china**
- **itu**
- **japan**

Usage

Use this command to select the national standard protocols to associate with the GTT process database.

Example

The following command sets the variant to *ansi*:

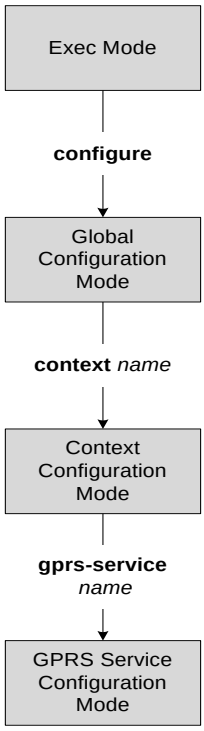
```
variant ansi
```

Chapter 130
GPRS Service Configuration Mode Commands

The GPRS Service Configuration Mode is used within the context configuration mode to define the criteria the SGSN needs to operate within a GPRS network. The GPRS Service works with other services, such as SGSN GPRS Tunneling Protocol (see SGTP Service Configuration Mode Commands) and Mobile Application Part (see MAP Service Configuration Mode Commands), to handle communication parameters required to work with other network entities such as the base station subsystem (BSS).

The prompt for this mode appears as:

```
[context_name]hostname(config-gprs-service)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

accounting

Defines the accounting context name and enables/disables specific types of CDR generation for the accounting in the GPRS service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

accounting { cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr } + | context *cntx_name* **}**

default accounting cdr-types

no accounting (cdr-types | context }

default

Returns the system to default CDR generation which includes M-CDR, S-CDR, and SMS CDRs.

no

Disables all CDR types.

cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr }

Default: all types enabled.
Defines the types of CDRs to be generated within the specified GPRS service for accounting:

- **mcdr:** Enables generation of M-CDRs.
- **scdr:** Enables generation of S-CDRs.
- **sms:** Enables generation of SMS-type CDRs based on one of the following:
- **mo-cdr:** SMS CDRs originates from the mobile.
- **mt-cdr:** SMS CDRs terminates at the mobile.

+

This symbol indicates that more than one keyword can be used and repeated. This enables you to include more than one type of CDR selection in a single command.

context *cntx_name*

Specifies an accounting context to be associated with the GPRS service.
cntx_name: Define a string of 1 to 79 alphanumeric characters.

Usage

Use this command to define the type of CDRs to generate for GPRS service. By default all types of CDRs are generated. Note that change of this configuration will be applied to new calls and/or to new PDP contexts only.
By default, generation of the S-CDR, M-CDR, SMS-MT-CDR, and SMS MO-CDR types is enabled.

Example

The following command configures the system to generate only M-CDRs for accounting in the current GPRS service:

```
accounting cdr-types mcdr
```

admin-disconnect-behavior

This command defines some of the actions the SGSN will take during an Admin-Disconnect procedure.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
admin-disconnect-behavior { clear-subscription | detach-type { reattach-not-required |
reattach-required } }

default admin-disconnect-behavior { clear-subscription | detach-type }
```

clear-subscription

Including this keyword in the configuration instructs the SGSN to clear subscriber contexts and the subscription data database whenever the **clear subscribers all** command is issued (from the Exec mode) for attached subscribers. As well, the SGSN will issue an appropriate Map-Purge-MS-Req to the HLR if needed.
Default: disabled

detach-type

Including this keyword defines which type of detach instruction to include in the Detach-Request message during an Admin-Disconnect procedure. One of the following options must be included when this command is entered:

- **reattach-not-required**
- **reattach-required**

Default: reattach-required

default

Including the **default** keyword in the command, instructs the SGSN to use the default value for the specified parameter.

no

Returns the SGSN to the default where this clear function is disabled

Usage

Using he **clear subscribers all** command (in the Exec Mode) will clear subscriber contexts and the subscription data database, and if needed, issue an appropriate Map-Purge-MS-Req to the HLR.
Include the **clear-subscription** keyword with this command configuration to ensure that more than attached MM-context and active PDP-contexts are cleared when the clear **subscribers all** command is issued for attached subscribers.
To clear subscription data for detached subscribers, refer to the **sgsn clear-detached-subscriptions** command described in the *Exec* mode chapter.

Including the **detach-type** keyword with this command instructs the SGSN to include either a 'reattach-required' or a 'reattach-no-required' instruction in the Detach-Request message.

Example

Enable the clearing function so that subscription data is cleared from the HLR database:

```
admin-disconnect-behavior clear-subscription
```

associate-dscp-template

Identifies a DSCP template to be associated with the GPRS service.

Important: This command can be used before the associated DSCP template instance is created and configured but care should be used to match the template names.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

associate-dscp-template downlink *template_name*

no associate-dscp-template downlink

no

Removes the template association definition from the configuration.

template_name

Specifies a unique DSCP template to associate with this GPRS service.
template_name must be a string of 1 to 64 alphanumeric characters with dots (.), dashes (-), and forward slashes (/) but with no spaces.

Usage

Use this command to associate DSCP templates with this GPRS service. A single template can be associated with multiple GPRS services.

Related commands:

- The dscp-template command in the SGSN Global configuration mode creates / deletes an instance of a template. This command also provides access to the mode containing all the configuration commands used to define DSCP settings for the control packets and data packets for a particular GPRS service (see the *DSCP Template Configuration Mode Commands* section).
- To check the list of DSCP templates configured, use the **show sgsn-mode** command documented in the *Exec Mode Commands* section.

Example

The following command associates the template with DSCP settings for traffic going through one of the SGSNs located in Paris mobile network:

associate-dscp-template *dscp-template-paris3*

associate-service

Identifies services to be associated with the GPRS Service.

Important: This command can be used before the associated service instance is created and configured but care should be used to match the service names.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] associate-service { gs *name* **| map** *name* **| sgtp** *name* **} [context** *ctxt_name* **]**

no

Removes the service association definition from the configuration.

gs *name*

Specifies the Gs service configuration to associate with this GPRS service.
name must be a string of 1 to 63 alphanumeric characters with no spaces.

map *name*

Specifies the MAP service configuration to associate with this GPRS service.
name must be a string of 1 to 63 alphanumeric characters with no spaces.

sgtp *name*

Specifies the SGTP service configuration to associate with this GPRS service.
name must be a string of 1 to 63 alpha numeric characters with no spaces.

context *ctxt_name*

Defines the context in which the service was created.
ctxt_name must be a string of 1 to 63 alphanumeric characters with no spaces.

Usage

Use this command to associate other services, that have been or will be configured, to this GPRS service.

Example

The following command associates Gs service *gs1* with this GPRS service.

```
associate-service gs gs1 context sgsn2
```

cc profile

Configures the charging characteristic (CC) profile index properties.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] cc profile *index* **{ buckets** *number* **| interval** *time* **| tariff time1** *mins hours* **[time2** *mins hours* **[time3** *mins hours* **[time4** *mins hours* **]]] | volume { downlink** *octets* **uplink** *octets* **| total** *octets* **} }**

default cc profile *index*

no

Removes the a specific charging characteristics configuration definition.

default

Resets the charging characteristics to system defaults.

index

Configures a profile index for the parameter to be specified. index can be configured to any integer value from 0 to 15.

Important: 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

buckets *number*

Default: 4
Specifies the number of statistics container changes due to QoS changes or tariff time that can occur before an accounting record should be closed.
number can be configured to any integer value from 1 through 4.

interval *time*

time is measured in seconds and can be configured to any integer value from 60 to 40,000,000.

tariff time1 *mins hours* **time2** *mins hours* **time3** *mins hours* **time4** *mins hours*

Specifies time-of-day time values to close the current statistics container (but not necessarily the accounting record). Six different tariff times may be specified. If less than six times are required, the same time can be specified multiple times.

Important: The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

For each of the different tariff times, the following parameters must be configured:

- *mins*: The minutes of the hour, an integer value from 0 to 59.
- *hours*: The hour of the day, an integer value from 0 to 23.

volume { downlink *vol_down_octets* **uplink** *vol_up_octets* **| total** *total_octets* **}**

Specifies the downlink, uplink, and total volumes that must be met before closing a CDR.
vol_down_octets : Measured in octets; can be configured to any integer value from 100,000 to 4,000,000,000.
vol_up_octets : Measured in octets; can be configured to any integer value from 100,000 to 4,000,000,000.
total_octets : The total traffic volume (up and downlink) measured in octets; can be configured to any integer value from 100,000 to 4,000,000,000.

Usage

Charging characteristics consist of a profile index and behavior settings. This command configures profile indexes for the SGSN's charging characteristics. The SGSN supports up to 16 profile indexes.
This command works in conjunction with the cc-sgsn command located in the APN configuration mode that dictates which CCs should be used for subscriber PDP contexts.

Example

The following command configures a profile index of 10 for tariff times of 7:00 AM and 7:30 PM:

```
cc profile 10 tariff time1 0 7 time2 30 19
```

check-imei

This command configures the action the SGSN will take if the route towards the EIR is down.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
check-imei { gf-failure-action | gf-timeout-action } { continue | reject }

default check-imei { gf-failure-action | gf-timeout-action }
```

default

Resets the default function to reject the Attach.

gf-failure-action

Coupled with either **continue** or **reject**, this keyword instructs the SGSN to take action if a valid EIR configuration exists under the MAP service and if the EIR is temporarily unreachable due to associated DPC/SSN inaccessible/out-of-service.

gf-timeout-action

Coupled with either **continue** or **reject**, this keyword instructs the SGSN to take action if a valid EIR configuration exists under the MAP service and the route to the EIR is available, but no response is received from the EIR.

continue

Instructs the SGSN to continue the Attach process.

reject

Instructs the SGSN to reject the Attach process.

Usage

Typically, the Attach process will be continued when there is an IMEI check timeout based on the configuration under the SGSN service configuration and/or the GPRS service configuration. But this works only if the route towards the EIR is UP and the IMEI request timer expires. This command configures the SGSN to allow the Attach process to continue in the case the route towards the EIR is down, that is the DPC / SSN is out-of-service.

Example

Use the following command to reset the default and reject Attach:

```
default check-imei gf-failure-action
```

check-imei-timeout-action

This command has been deprecated.

ciphering-algorithm

This command configures the priority, ordering, for the use of the GPRS encryption ciphering algorithms.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
ciphering-algorithm { negotiation-failure-action { reject [ failure-code cause_code ] |
use-geo0 } priority priority [ algorithm ]  }

default ciphering-algorithm priority priority
```

default

Returns the system ciphering-algorithm priority to the default of GEA0 - which means that no ciphering will be done.

negotiation-failure-action { reject [failure-code *cause_code*] | use-geo0 }

This set of keywords configure the SGSN's action if there is not a match between the MS and SGSN ciphering algorithm configurations.

- **reject**: Instructs the SGSN to reject a call when the ciphering algorithms do not match.
- **failure-code** *cause_code*: Instructs the SGSN to include a GMM cause code in the Reject message. Enter an integer from 2 to 111; default code is 14 (GPRS services not allowed in this PLMN). Refer to the GMM failure cause codes listed below (information has been taken from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):
  - 2 - IMSI unknown in HLR
  - 3 - Illegal MS
  - 6 - Illegal ME
  - 7 - GPRS services not allowed
  - 8 - GPRS services and non-GPRS services not allowed
  - 9 - MSID cannot be derived by the network
  - 10 - Implicitly detached
  - 11 - PLMN not allowed
  - 12 - Location Area not allowed
  - 13 - Roaming not allowed in this location area
  - 14 - GPRS services not allowed in this PLMN
  - 15 - No Suitable Cells In Location Area
  - 16 -MSC temporarily not reachable
  - 17 - Network failure
  - 20 - MAC failure

- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

- **use-geo0**: Instructs the SGSN to honor the Attach/RAU Request without ciphering (geo0). This is the default action for negotiation failure.

---

priority *priority algorithm*

Defines the priority, order of use, for the ciphering algorithm.
priority: Must be an integer from 1 to 4.

---

algorithm

Identifies the algorithm to be matched to the priority. Options include:

- gea0 - No ciphering
- gea1 - GPRS Encryption Algorithm - GEA1
- gea2 - GPRS Encryption Algorithm - GEA2
- gea3 - GPRS Encryption Algorithm - GEA3

Usage

Use this command to specify the order (priority) of usage for the GPRS encryption algorithms. All of the GPRS encapsulation algorithms use a 64-bit key derived from a common mechanism: the mobile receives a random challenge, then the SIM calculates an authentication signature and an encryption key.
Also use this command to define the action to be taken if there is not a match between the MS and the SGSN ciphering algorithm configurations.

Example

The following command sets no ciphering to be used after two encryption algorithms have been used:

```
ciphering-algorithm priority 3 gea0
```

The following command configures the SGSN to reject calls if the ciphering algorithm configurations don't match:

```
ciphering-algorithm negotiation-failure-action reject
```

dns israu-mcc-mnc-encoding

Configures either decimal or hexadecimal format for the MCC and MNC values in the DNS query.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
dns israu-mcc-mnc-encoding { decimal | hexidecimal }

default dns israu-mcc-mnc-encoding
```

default

Resets the SGSN to send the MCC and MNC values in decimal format for DNS queries.

decimal

Default.
Instructs the SGSN to send the MCC and MNC in decimal format in the DNS query.

hexadecimal

Instructs the SGSN to send the MCC and MNC in hexadecimal format in the DNS query.

Usage

Use this command to determine the type of encoding for the MCC and MNC to be included in the DNS query. For example:
In decimal, the MNC/MCC in a DNS query would appear like:

```
rac0017.lac42e3.mnc310.mcc722.gprs
```

In hexadecimal, the MNC/MCC in a DNS query would appear like:

```
rac0017.lac42e3.mnc0136.mcc02d2.gprs
```

Example

Use hexadecimal values for the MCC/MNC in the DNS query.

```
dns israu-mcc-mnc-encoding hexadecimal
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Return to the Exec mode.

exit

Exits the current configuration mode and returns to the previous configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the context configuration mode.

gmm

gmm actually provides a set of commands used to define the GPRS mobility management parameters for the SGSN service.

Important: The **gmm** commands can be repeated as needed to set each timer.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gmm { accept-procedure [new-tlli | old-tlli] | attach ptmsi-signature-mismatch send-reject failure-code *cause_code* **| ciph-gmm-msg-from-unknown-ms { detach | ignore } | mobile-reachable-timeout** *mins* **| negotiate-t3314-timeout** *secs* **| purge-timeout** *mins* **| T3302-timeout** *mins* **| T3312-timeout** *mins* **| T3313-timeout** *secs* **| T3350-timeout** *secs* **| T3360-timeout** *secs* **| T3370-timeout** *secs* **| trau-timeout***secs* **}**

default gmm { attach ptmsi-signature-mismatch | ciph-gmm-msg-from-unknown-ms | mobile-reachable-timeout | negotiate-t3314-timeout | purge-timeout | T3302-timeout | T3312-timeout | T3313-timeout | T3350-timeout | T3360-timeout | T3370-timeout | trau-timeout }

no gmm negotiate-t3314-timeout

default

Disables the specified function or resets the specified timer to system defaults.

no

Removes the specified GMM definition from the configuration.

accept-procedure [new-tlli | old-tlli]

Default: new-tlli
This keyword enables the use of either a new TLLI (temporary logical link identifier) or an old TLLI for attach-accept or RAU-accept messages sent by the SGSN to the MS during related procedures.

attach ptmsi-signature-mismatch send-reject failure-code *cause_code*

Default: disabled
This keyword enables the SGSN to validate the P-TMSI signature, present in the Attach Request, against the PTMSI-SIGNATURE stored at the SGSN. The SGSN then sends an Attach Reject to the MS if the PTMSI-SIGNATURE does not match.
The P-TMSI signature validation functionality only works if the feature is enabled. But even if it is enabled, the feature does not validate in the following situations:

- when the PTMSI-SIGNATURE is absent from the 2G Attach Request.
- if the first subscriber being in DETACHED state or is purged with FREEZE-PTMSI. In both the scenarios PTMSI-SIGNATURE cannot be validated.

- when the 2G subscriber(MS2) attaches with the same P-TMSI and a different P-TMSI_Signature as previously attached 2G subscriber (MS1), both the subscriber profiles are cleared from the system. This is relevant where the old RAI for MS-2 is the same as the current RAI for MS-1.

Optionally, a GMM failure *cause_code* can be configured to include in the Attach Reject if one is sent. Refer to the GMM failure cause codes listed below (information has been taken from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

---

ciph-gmm-msg-from-unknown-ms { detach | ignore }

Configures how the SGSN will behave when it receives a ciphered GMM message from an unknown MS.
detach - Instructs the SGSN to send a Detach message to the MS.
ignore - Instructs the SGSN to send an Ignore (drop) message to the MS.
Default: **ignore**

mobile-reachable-timeout *mins*

Default: 58 minutes
Timer value for the mobile reachability timer.
mins must be an integer from 4 to 1440.

negotiate-T3314-timeout *secs*

Set the number of seconds for the T3314-timeout ready timer value. Value sent out from SGSN so MS can negotiate ready timer.
secs must be an integer from 0 to 11160. Default is 44 seconds.

- If the MS does not send the ready timer in the Attach/RAU request, then the SGSN sends this T3314-timeout (ready timer) value.
- If the MS sends the requested value of the ready timer in the Attach/RAU Request, and if the requested value is less than or equal to the value of the negotiate-T3314-timeout timer, then the SGSN sends Att/RAU Accept with the requested T3314 value.
- If the MS sends the requested value of the ready timer in the Attach/RAU Request, and if the requested value is greater than the value of the negotiate-T3314-timeout timer, then the SGSN sends Att/RAU Accept with the negotiate-T3314-timeout value.

Important: This is the only GMM timer that can be disabled by entering **no** at the beginning of the command syntax. **no gmm negotiate-t3314-timeout** By disabling negotiation of the T3314-timeout value, if the MS sends the requested value of the ready timer in the Att/RAU Request, then the SGSN sends the T3314-timeout value in the Att/RAU Accept.

purge-timeout *mins*

Default: 10080 minutes
Value defines the mm-context lifetime in minutes.
mins must be an integer from 1 to 20160.

T3302-timeout *mins*

Default: 12 minutes
Defines the number of minutes for timer to send to MS.
mins is an integer from 1 to 186.

T3312-timeout *min*

Default: 54 minutes
Periodic RAU update timer to send to MS.
mins is an integer from 0 to 186.

T3313-timeout *secs*

Default: 5 seconds
Initial page timeout timer for retransmission for Paging Requests.
secs is an integer from 1 to 60.

T3314-timeout *secs*

Default: 44 seconds
Ready Timer for controlling Cell Update Procedure.

secs must be an integer from 0 to 11519.

T3350-timeout *secs*

Default :6 seconds
Retransmission timer for Attach Accept/RAU Accept/P-TMSI Realloc Command.
secs must be an integer from 1 to 20.

T3360-timeout*secs*

Default :6 seconds
Retransmission timer for Authentication Request.
secs must be an integer from 1 to 20.

T3370-timeout *secs*

Default :6 seconds
Retransmission timer for Identity Request.
secs must be an integer from 1 to 20.

trau-timeout *secs*

This timer is available in releases 9.0 and higher.
Default: 30
Specifies the number of seconds the "old" 3G SGSN waits to purge the MS's data. This timer is started by the "old" SGSN after completion of the inter-SGSN RAU.
secs : Must be an integer from 5 to 60.

Usage

Use this command to set GMM timers.

Example

Set the t3370 timer expiration for 15 seconds:

```
gmm t3370-timeout 15
```

llc

Configures the timers that control the data flow for the logical link control (LLC) sub-layer.

Important: This command may be repeated as often as necessary to define the needed timers.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

llc { iov-ui-in-xid-reset | n201u-max { sapi11 *pkt-size* **| sapi3** *pkt-size* **| sapi5** *pkt-size* **| sapi9** *pkt-size* **} | nu-overflow-detection high-watermark** *high_num* **low-watermark** *low_num* **increment-oc| pdu-lifetime** *secs* **| reset-vur | t200 sapi1** *time* **| t200 [sapi11** *time* **| sapi3** *time* **| sapi5** *time* **| sapi7** *time* **| sapi9** *time* **] | uplink-pdu-len-validation }**

default llc { iov-ui-in-xid-reset | n201u-max { sapi11 | sapi3 | sapi5 | sapi9 } | nu-overflow-detection | pdu-lifetime | reset-vur | T200 [sapi1 | sapi11 | sapi3 | sapi5 | sapi7 | sapi9] | uplink-pdu-len-validation }

no llc { iov-ui-in-xid-reset | nu-overflow-detection | reset-vur | uplink-pdu-len-validation }

default

Resets the configuration to the default values.

no

Disables the **uplink-pdu-len-validation** .

iov-ui-in-xid-reset

This keyword makes it possible for the operator to configure whether or not to send IOV-UI in an XID-RESET. This is useful when the MS is not setup to accept IOV-UI (for example, MS sends Attach/RAU Requests with cksn=7) and including IOV-UI in the XID-Reset would result in Attach/RAU failure.
Default: Enabled

n201u-max sapi *n* *pkt_size*

This keyword sets the maximum number of octets, per service access point identifier (SAPI), for the downlink data packets. This is the upper limit that the SGSN will negotiate with the subscriber for packets sent from the SGSN to the BSC.
sapi *n* : Command must identify one of the following SAPI: sapi11, sapi3, sapi5, or sapi9.
pkt_size : Must be an integer from 140 to 1520. Default size is 1520 octets.

nu-overflow-detection high-watermark *high_num* **low-watermark** *low_num* **increment-oc**

Enables/disables overflow detection for the N(u) counter and setting overflow high/low thresholds facilitates ciphering synchronization between the MS and SGSN.

high_num: Enter an integer between 1 and 511.
low_num: Enter an integer between 0 and 510.
If the expected value of nu(Vur) is greater than or equal to the configured high-watermark, and the received nu(LFN) is less than or equal to the configured low-watermark, the SGSN increments the overflow counter (VurOC).
The recommended overflow settings are as follows:**llc nu-overflow-detection high-watermark 496 low-watermark 15 increment-oc** While expecting a packet with 496 < nu < 511 and a packet with 0 < nu < 15 is received, overflow is detected and VurOC is incremented.

---

pdu-lifetime *secs*

Defines LLC layer PDU lifetime at the BSC. .
secs must be an integer from 0 to 90.
Default: 6

---

reset-vur

Enables/disables the mechanism to reset the Vur value maintained at LLC if the intra RAU request is received with N(U) = 0
Default: Disabled

T200 sapi1 *time*

Sets the retransmission timer (in seconds) for sapi1.
time must be an integer of 1 to 10.
Default: 5

T200 sapi11 *time*

Sets the retransmission timer (in seconds) for sapi11.
time must be an integer of 1 to 50.
Default: 40

T200 sapi3 *time*

Sets the retransmission timer (in seconds) for sapi3.
time must be an integer of 1 to 10.
Default: 5

T200 sapi5 *time*

Sets the retransmission timer (in seconds) for sapi5.
time must be an integer of 1 to 20.
Default: 10

T200 sapi7 *time*

Sets the retransmission timer (in seconds) for sapi7.
time must be an integer of 1 to 40.
Default: 20

T200 sapi9 *time*

Sets the retransmission timer (in seconds) for sapi9.
time must be an integer of 1 to 40.
Default: 20

uplink-pdu-len-validation

Available in releases 8.1 and higher.
This feature enables validation of the size of the uplink LLC packets. With validation enabled, the SGSN will drop any uplinked packets that are larger than the negotiated limit.
If the **no** form of the command is used, then this feature is disabled. The SGSN will be more flexible with uplink packet sizes. So if the SGSN and MS have a mismatch and the MS sends packets that are larger than expected, then the SGSN will not drop the packets.
Default: Enabled.

Usage

Use the command repeatedly to configure additional timers and features for the LLC sub-layer.

Example

Set the T200 retransmission timer to timeout at 12 seconds for SAPI5:

```
llc t200 sapi5 12
```

Use the following command to instruct the SGSN to ignore the N201_U packet size limits for uplink packets from an MS:

```
no uplink-pdu-len-validation
```

nri

This command configures the network resource identifier (NRI) to identify a specific SGSN. The NRI is stored in the P-TMSI. The SGSN uses a portion of this NRI to set the parameters for Gb flex (SGSN pooling) functionality.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

nri length *nri_length* **{ nri-value** *nri_value* **| null-nri-value** *null_nri_value* **non-broadcast-lac** *lac_id* **rac** *rac_id* **[nri-value** *value* **}**

no nri

---

no

Removes the configured NRI value and location in P-TMSI for retrieval by this SGSN operator policy.

---

nri length *nri_length*

Specifies the number of bits to be used in the P-TMSI, bits 23 to 18. to define the network resource identifier (NRI). The NRI length configuration also sets the maximum size of the pool. If not configured, the NRI length will be of zero length.
nri_length : Must be an integer from 1 to 6 to identify the number of bits.

---

null-nri-value *null_nri_value*

Configures the null NRI value which must be unique across the pool areas. This keyword is used for the offloading procedure for SGSN pooling (enabled with the **sgsn offloading** command, see the *Exec Mode* chapter).
null_nri_value : 0 (zero) indicates the keyword is not to be used and 1 to 63 are used to identify the SGSN to be used for the offloading procedure for SGSN pooling. There is no default value for this parameter.

---

non-broadcast lac *lac_id* **rac** *rac_id*

Defines the non-broadcast LAC/RAC to be used in combination with the null-NRI for the offloading procedure.
lac_id defines a location area code associated with a BSS. Must be an integer between 1 and 65535.
rac_id defines the remote area code to be associated with a BSS. Must be an integer between 1 and 255.

---

nri-value *nri_value*

Specifies the MS-assigned value of the NRI to retrieve from the P-TMSI. This value must not exceed the maximum possible value specified by the NRI length. The NRI value must be unique across the pool or across all overlapping pools.
nri_value must be an integer from 1 to 63 to identify a specific SGSN in a pool. Use of 0 (zero) value is not recommended.
Multiple NRI values can be identified by providing multiple nri-values separated by a blank space for example: **nri length** *6* **nri-value** *29 43 61*

Usage

Use this command to add or remove the Gb flex pool configuration for this GPRS service. The command can be repeated to specify different values for any of the keyword parameters. If more than one NRI is configured, the GPRS service will round-robin between the available NRIs when new subscribers (re)connect.

Use this command to retrieve the NRI (identity of an SGSN) stored in in bits 23 to 18 of the packet-temporary mobile subscriber identity (P-TMSI). If more than one NRI value is configured, the GPRS service will round-robin between the available NRIs when new subscribers (re)connect.

Example

The following command specifies the the NRI length as 5 bits, identifies SGSN 23 with LAC 222 and RAC 12 for offloading procedure with NRIs 6 and 41:

```
nri length 5 null-nri-value 34 non-broadcast lac 222 rac 12 nri-value 6
41
```

paging-policy

Configures the paging parameters for the GPRS service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
paging-policy { last-known-area { all | bsc | cell | location-area | routing-area } + |
max-retransmissions retran_num }

no paging-policy last-known-area { bsc | cell | location-area | routing-area }

default paging-policy { last-known-area | max-retransmissions }
```

no

Disables the paging-policy definition for this GPRS service configuration.

default

Resets the defaults for parameters managed by this paging policy.

last-known-area

Select one or more paging areas and enter them in preferred paging order:

- **all** : Pages in the last known BSC.
- **bsc** : Pages in last known BSC.
- **cell** : Pages in last known cell.
- **location-area** : Pages in last known location area.
- **routing-area** : Pages in last known routing area.

By default, paging occurs in the following order:
cell, BSC, routing area, location area.

max-retransmission *retran_num*

Configures the maximum number of retries for a page request per paging area.
retran_num: Enter an integer from 0 to 5.

- 2 : default.
- 0 : disables retransmission for paging request so that the SGSN only sends a single 2G PS-paging request to the BSC with no retransmissions.

+

Keywords can be repeated or combined as needed to complete the paging policy configuration.

Usage

Use this command to configure the order of preference for retransmitting into specified paging-areas.

Example

Use the following command to instruct the SGSN to page the cell and BSC as the last-known areas :

```
paging-policy last-known-area cell bsc
```

peer-nsei

This command associates a peer (remote) network service entity (NSEI) for a BSS with this GPRS service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
peer-nsei nse_id  { lac lac_id rac rac_id | pooled }

[ no ] peer-nsei nse_id { lac lac_id rac rac_id  | pooled }
```

no

Removes the NSEI LAC/RAC or pooling configuration from this BSS peer configuration.

nse_id

Defines the NSEI for this GPRS service.
nse_id must be an integer from 0 to 65535.

lac *lac_id*

Defines a location area code associated with the NSE BSS.
lac_id must be an integer between 1 and 65535.

rac *rac_id*

Defines the remote area code to be associated with the NSE BSS
rac_id must be an integer between 1 and 255.

pooled

Enables pooling with non-pooled BSCs within the pool area.

Usage

Use this command repeatedly to associate one or more LAC/RAC combinations and/or pooling with this peer-GPRS service configuration.
The Network Service Entity (NSE) at the BSS and the SGSN provides the network management functionality required for the operation of the Gb interface. Each NSE is identified by means of NSE identifier (NSEI).

Example

The following command configures the NSE with identifier as *4114* having location area code *234* and routing area code as *22*:

```
peer-nsei 4114 lac 234 rac 22
```

The following command enables Gb flex (pooling) functionality for this GPRS service:

```
peer-nsei 4114 pooled
```

plmn

This command identifies the Public Land Mobile Network (PLMN) for the GPRS service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

plmn id mcc *mcc_num* **mnc** *mnc_num*

no plmn id

no

Removes the PLMN information from the configuration for the current SGSN service.

mcc *mcc_num*

Define the mobile country code (MCC) portion of the PLMN Id.
mnc_num must be a 3 digit integer from 100 to 999.

mnc *mnc_num*

Define the mobile network code (MNC) portion of the PLMN Id.
mnc_num must be a 2 or 3 digit integer from 00 to 999.

Usage

Use this command to set PLMN parameters for the current SGSN service.

Example

The following command identifies the PLMN MCC as 200 and the MNC as 10:

```
plmn id mcc 200 mnc 10
```

reporting-action event-record

This command enables the SGSN to log GMM/SM events in EDR files for 2G services.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
reporting-action event-record

[ default | no ] reporting-action event-record
```

default

Disables the logging function.

no

Removes the logging function from the configuration file.

Usage

This command is one of the steps needed to enable the SGSN to create a log for events such as Attach, RAU, and Activations. The log is an EDR (event data record) in CSV format. For details about how this feature works, refer to the *GMM-SM Event Logging* chapter in the *SGSN Administration Guide*.

Related Commands:

- To enable GMM/SM event logging for 2G services, the **reporting-action event-record** command must be configured in the SGSN service configuration.
- To enable a log to be generated in an EDR file, the **edr-module active-charging-service** command must be enabled in the Context configuration mode.
- To configure parameters for the logging file characteristics and for file transfer, use the commands in the EDR Module Configuration Mode.

Example

Enable GMM/SM event logging for 3G services:

```
reporting-action event-record
```

setup-timout

This command configures the maximum number of seconds allowed for session setup.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

setup-timout *seconds*

default setup-timout

default

Returns the configuration to the default, 60 seconds.

seconds

An integer from 1 to 1000000.

Usage

Use this command to set the time allowed for session setup.

Example

The following command sets the maximum session setup time to 300 seconds:

setup-timout *300*

sgsn-context-request

This command specifies whether or not the PTMSI signature check should be skipped if the PTMSI signature is not included in the SGSN context request.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
sgsn-context-request ptmsi-signature-absence allowed

default sgsn-context-request ptmsi-signature-absence

no sgsn-context-request ptmsi-signature-absence allowed
```

default

Returns the configuration to the default action to perform the PTMSI signature check.

no

Removes this definition from the system configuration.

Usage

Use this command to skip the PTMSI signature check.

Example

The following command instructs the system to perform the PTMSI signature check.

```
default sgsn-context-request ptmsi-signature-absence
```

sgsn-number

Define the SGSN E.164 number to be used when interacting via MAP protocol for this GPRS service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sgsn-number *sgsn_number*

no sgsn-number

no

Disables the use of this definition in the system configuration.

sgsn-number

Enter a string of 1 to 16 digits to identify the SGSN's E.164 identification.

Usage

Use this command to identify the ISDN number for the SGSN associated with this GPRS service.
The SGSN supports multiple SGSN numbers – different numbers in the 2G GPRS service configuration and the the 3G SGSN service configuration. If an HLR-initiated dialog is received, the SGSN will perform a lookup based on the IMSI and find the correct SGSN number with which the MS is associated. Subsequent messaging will use this address.

Example

Disable the E.164 number for this GPRS service.

```
no sgsn-number
```

sm

This command configures the session management (SM) parameters associated with this particular GPRS service context.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sm { activate-max-retransmissions *num_retries* **| deactivate- max-retransmissions** *num_retries* **| ignore-pco-decode-error | modify-max-retransmissions** *num_retries* **| partial-apn-match | requested-apn-from-first-subrec | t3385-timeout** *secs* **| t3386-timeout** *secs* **| t3395-timeout** *secs* **| trim-trailing-spaces-in-apn }**

default sm { activate-max-retransmissions | deactivate-max-retransmissions | ignore-pco-decode-error | modify-max-retransmissions | t3385-timeout | t3386-timeout | t3395-timeout | trim-trailing-spaces-in-apn }

default

Resets the SM parameters to the defaults.

activate-max-retransmissions *num_retries*

Defines the maximum number of retries to transmit 'activate PDP context request'.
num_retries : Must be an integer from 1 to 10.
Default: 4

deactivate-max-retransmissions *num_retries*

Defines the maximum number of retries to transmit 'deactivate PDP context request'.
num_retries : Must be an integer from 1 to 10.
Default: 4

ignore-pco-decode-error

Enables the SGSN to ignore received decode errors that are due to incorrectly encoded PCO IE length in SM Requests.
Default: disabled

modify-max-retransmissions *num_retries*

Defines the maximum number of retries to transmit 'modify PDP context request'.
num_retries: integer from 1 to 10.
Default: 4

partial-apn-match

Enables partial matching of requested APN during APN selection.

Partial APN or APN with trailing spaces may be present in an Activate Request because incorrect information was keyed in by the user. Though it is valid to reject such Activation Requests, it increases the signaling between the MS and the SGSN. This has an impact on the radio resources.

requested-apn-from-first-subrec

Enables use of a 'requested APN' from the first subscription record. When this feature is enabled, the PDP Activation is not rejected during APN Selection; instead, the APN from the first subscription record is used as the requested APN and the SGSN continues with the rest of the APN Selection process.
A requested APN is an optional IE in an Activate PDP Request. To get the requested PDP type, if multiple PDP subscription records exist for the subscriber, then the MS has to include the APN information to choose the PDP subscription record during APN selection. Otherwise, such activations will be rejected during APN selection (per TS 23.060 Appendix A). Though it is valid to reject such activation requests, it increases the signaling between the MS and the SGSN, which impacts the radio resources.

t3385-timeout*secs*

Defines the maximum amount of time for retransmission of 'activate request' messages.
secs : Must be an integer from 1 to 60.
Default: 8

t3386-timeout *secs*

Defines the maximum amount of time for retransmission of 'modify request' messages.
secs : Must be an integer from 1 to 60.
Default: 8 seconds.

t3395-timeout *secs*

Defines the maximum amount of time for retransmission of 'deactivate request' messages.
secs : Must be an integer from 1 to 60.
Default: 8

trim-trailing-spaces-in-apn

Enables SGSN to strip off any trailing space(s) in requested APN.
If a requested APN in an Activate PDP Context Request has any trailing spaces, then those trailing spaces will be removed and the length field will be updated.

Usage

Repeat this command with different keywords (parameters) to configure the SM (session management) as needed for this GPRS service. Keywords can be used to optimize signaling between the MS and the SGSN to reduce the impact on the radio resources.

Example

Reset the number of retransmission messages for deactivate PDP context request to 5.

```
sm deactivate-max-retransmissions 5
```

sndcp

Define the sub-network dependent convergence protocol (SNDCP) network packet data unit (N-PDU) reassembly timeout interval associated with this GPRS service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sndcp reassembly-timeout *seconds*

default sndcp reassembly-timeout

default

Resets the timer configuration to the default value of 30 seconds.

seconds

Defines the the number of seconds the SGSN waits for all the SNDCP segments to arrive before dropping all the disassembled segments.
seconds: Must be an integer from 1 to 300.

Usage

Use this command to modify the SNDCP reassembly timer. This timer starts as soon as the first N-PDU segment is received (either in-order or out-of-order). If all the segments belong to the N-PDU arrive before the timer expires then the segments are reassembled. If all the segments do not arrive before the timer expires, then the stored segments are discarded.

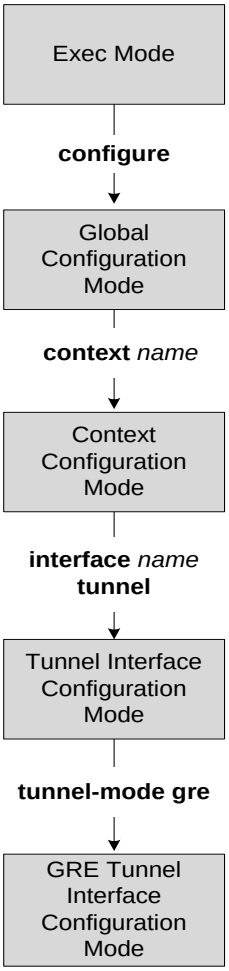
Example

Reset the default for the timer.

```
default sndcp reassembly-timeout
```

Chapter 131
GRE Tunnel Interface Configuration Mode Commands

The Generic Routing Encapsulation (GRE) Tunnel Interface Configuration Mode is used to create and manage the GRE tunneling interfaces for addresses, address resolution options, etc.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

destination

This command configures the destination IP address of the tunnel by specifying the destination end address. This is a mandatory configuration for a GRE tunnel interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] destination address ip_address
```

no

Removes or disassociates the configured destination IP address from a specific GRE tunnel interface configuration.

address *ip_address*

Configures the IP address for the interface.
ip_address must be specified using the IPv4 dotted-decimal notation.

Usage

Use this command to configure the destination IP address of the tunnel by specifying the IP address of destination tunnel end for GRE tunnel interface.

Important: State of source address will affect the operational state of the tunnel.

Example

The following command sets the 10.2.3.4 as destination IP address of the GRE tunnel interface:

```
destination address 10.2.3.4
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

keepalive

This command configures various parameters for sending Keepalive messages to the remote end-point in GRE tunnel interface configuration. By default sending keepalives is disabled.

Product

All

Privilege

Security Administrator, Administrator

Syntax

keepalive [interval *time_interval* **num-retry** *retry*]

[default | no] keepalive

default

Sets the sending of Keepalives with default parameters.
interval: 10 seconds
num-retry: 3 retries

no

Disables the keepalive and turns off the sending of Keepalives messages.

interval *time_interval*

Default: 10
Specifies the time interval (in seconds) between two Keepalives sent to remote ends of GRE tunnel interface configuration.
time_interval must be an integer from 5 through 3600.

num-retry *retry*

Default: 3
Specifies number of retransmission of keepalives to remote node without getting any response before the remote node is marked as dead/down.
retry must be an integer between 0 through 10.

Usage

Use this command to configure the parameters for sending Keepalives to the remote end-point of GRE tunnel. It also configures the interval at which GRE Keepalives are sent on the interface and number of retries without getting a response from the remote end-point before the tunnel is shutdown. By default, Keepalives will not be sent.

Example

The following command enables the keepalive and sets the other parameters to defaults:

```
default keepalive
```

source

This command configures the source IP address of the tunnel either by specifying the IP address (host address) or by specifying another configured non-tunnel IP interface. This is a mandatory configuration for GRE tunnel interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] source {address ip_address | interface interface_name}
```

no

Removes/disassociates the configured source IP address or host interface from a specific GRE tunnel interface configuration.

address *ip_address*

Configures the IP address for the interface specifying the IP address.
ip_address must be specified using IPv4 dotted-decimal notation.

interface *interface_name*

Specifies the name of the preconfigured non-tunnel IP interface, whose address is used as the source address of the GRE tunnel.

Usage

Use this command to configure the source IP address of the tunnel either by specifying the IP address (host address) or by specifying another configured non-tunnel IP interface for GRE tunnel interface.

Important: State of source address will affect the operational state of the tunnel.

Example

The following command sets the 10.2.3.4 as source IP address of the GRE tunnel interface:

```
source address 10.2.3.4
```

tos

This command configures the parameters/action for the type of Service (ToS) parameter in the IP tunnel transport protocol header.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
ip tos {value [ af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 |
af42 | af43 | be | ef | lower-bits tos_value] | copy}

no ip tos
```

default

Sets the IP TOS to lower bits value of 0.

value [*tos_value***]**

Default: **af11**
Specifies the IP QoS DSCP per-hop behavior to be marked on the outer header of signalling packets originating from the Access Gateway. This is a standards-based feature (RFC 2597). The following forwarding types are supported:

- **af11**: Assured Forwarding 11 per-hop behavior
- **af12**: Assured Forwarding 12 per-hop behavior
- **af13**: Assured Forwarding 13 per-hop behavior
- **af21**: Assured Forwarding 21 per-hop behavior
- **af22**: Assured Forwarding 22 per-hop behavior
- **af23**: Assured Forwarding 23 per-hop behavior
- **af31**: Assured Forwarding 31 per-hop behavior
- **af32**: Assured Forwarding 32 per-hop behavior
- **af33**: Assured Forwarding 33 per-hop behavior
- **af41**: Assured Forwarding 41 per-hop behavior
- **af42**: Assured Forwarding 42 per-hop behavior
- **af43**: Assured Forwarding 43 per-hop behavior
- **be**: Best Effort forwarding per-hop behavior
- **ef**: Expedited Forwarding per-hop behavior typically dedicated to low-loss, low-latency traffic.

The assured forwarding behavior groups are listed in the table below.

	Class 1	Class 2	Class 3	Class 4
Low Drop	AF11	AF21	AF31	AF41

	Class 1	Class 2	Class 3	Class 4
Medium Drop	AF12	AF22	AF32	AF42
High Drop	AF13	AF23	AF33	AF43

Traffic marked with a higher class is given priority during congestion periods. If congestion occurs to traffic with the same class, the packets with the higher AF value are dropped first.

lower-bits *tos_value*

Default: 0
Sets the least-significant 6 bits in the ToS byte with the specified numeric value.
tos_value must be an integer from 0 through 255.

copy

This keyword instructs the system to copy the ToS value from the passenger IPv4 packet or Traffic class value from the passenger IPv6 packet to the ToS value of the IPv4 tunnel transport protocol header

Usage

Use this command either to set the ToS parameter in the IPv4 tunnel transport protocol header to the specified value or instructs to copy the ToS value from the passenger IPv4 packet or Traffic class value from the passenger IPv6 packet to the ToS value of the IPv4 tunnel transport protocol header. If one of the enumerated values is set, the DSCP bits which are the six most-significant bits in the ToS byte are marked. If the integer value is set, it will be written into the six least-significant bits of the ToS byte.

Example

The following command instructs the system to copy the ToS value from the passenger IPv4 packet or Traffic class value from the passenger IPv6 packet to the ToS value of the IPv4 tunnel transport protocol header:

```
tos copy
```

ttl

This command configures the Time to live (TTL) parameter to be used in the tunnel transport protocol header for the current GRE tunnel interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ttl *ttl_value*

default ttl

default

Sets the TTL value to system default value.

ttl_value

Default: 15
Specifies the maximum time to live to be used in the tunnel transport protocol header
The time to live (TTL) is not a measure of time but the number of hops through the network.
ttl_value must be an integer between 1 through 255.

Usage

Use this command to set the TTL parameter to be used in the tunnel transport protocol header for the GRE tunnel configuration.

Example

The following configures the TTL to a value of *10*:

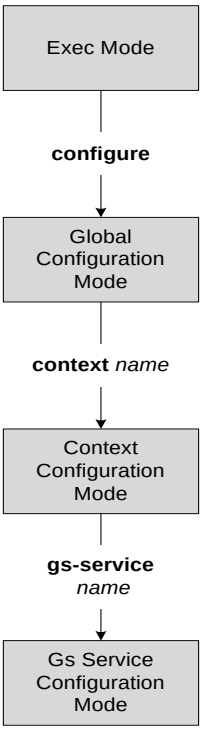
```
ttl 10
```

Chapter 132
Gs Service Configuration Mode Commands

The Gs Service configuration mode configures the parameters used to setup and maintain a Gs interface for a connection between the SGSN and an MSC/VLR.

Upon accessing this mode, your prompt should look similar to the following:

```
[<context_name>]<hostname>(config-gs-service)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

associate-sccp-network

This command associates a previously defined Signaling Connection Control Part (SCCP) network instance with the Gs service. This association is required to access Visitor Location Register(s) (VLRs).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

associate-sccp-network *sccp_net_id*

no associate-sccp-network

no

Removes the associated SCCP network configuration instance from this Gs service configuration.

sccp_net_id

Identifies the SCCP network configuration instance to associate with this Gs interface to enable connection with VLR(s).
sccp_network_num: Must be an integer from 1 through 12.

Usage

Use this command to associate the SCCP network configuration instance with the Gs interface in this service.

Important: A single SCCP network configuration instance can not be shared with multiple Gs services.

Important: To enable a Gs service, the user needs to configure **ssn** with the **bssap+** command.

Example

Following command associates SCCP network 2 with this Gs service.

associate-sccp-network *2*

bssap+

This command defines the Base Station System Application Part Plus configuration parameters for the Gs service to enable the SGSN to access a Visitor Location Register(s) (VLRs).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

bssap+ ssn *ss_num*

no bssap+ ssn *ss_num*

no

Removes the configured BSSAP+ subsystem number from this Gs service.

ssn *ss_num*

Specifies the subsystem number to configure in this Gs interface to use BSSAP+.
ss_num must be an integer from 1 through 255.

Usage

Use this command to configure the BSSAP+ subsystem with Gs interface in this service to communicate with VLR(s).

Important: A single SCCP network configuration instance can not be shared with multiple Gs services.

Important: To start a Gs service, the user needs to configure the command parameter.

Example

Following command configures subsystem 101 with BSSAP+ in this Gs service.

bssap+ ssn *101*

end

Exits the current configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Return to the Exec mode.

exit

Exits the current configuration mode and returns to the previous configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Return to the previous configuration mode.

max-retransmission

This command configures the retransmission values for different procedure counters in Gs service as described in TS 29.018.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

max-retransmissions { n8 | n9 | n10 | n12 } *retrans_num*

default max-retransmissions { n8 | n9 | n10 | n12 }

no

Removes the configured Gs procedures from this Gs service.

{ n8 | n9 | n10 | n12 }

Specifies the various Gs service procedures that are available to be used to communicate with VLR(s).

- n8: Defines the maximum number of retries for explicit IMSI detach from a non-GPRS service. Default is 2.
- **n9**: Defines the maximum number of retries for explicit IMSI detach from a non-GPRS service. Default is 2.
- **n10**: Defines the maximum number of retries for implicit IMSI detach from the GPRS service. Default is 2.
- **n12**: Defines the maximum number of retries for BSSAP+ to send Reset Indication messages. Default is 2.

retrans_num

Default: 2
Specifies the number of re-transmission of message for specified procedures.
retrans_num: Must be an integer from 0 through 10.

Usage

Use this command to configure the retransmission values for specific procedure counters in Gs service. counters are based on TS 29.018.
This command can be entered for each procedure counter separately.

Example

Following command configure retransmission value as *3* for counter for procedure to send BSSAP+ Reset Indication messages in this Gs service.

```
max-retransmissions n12 3
```

non-pool-area

This command creates a non-pool area for a set of subscriber location area code (LAC) values that can be used with a specific VLR for the Gs service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

non-pool-area *non_pool_name* **{ use-vlr** *vlr_name* **lac** *lac_num* **} +**

no non-pool-area *non_pool_name* **[lac** *lac_num*

no

Removes the configured non-pool area from this Gs service.

non_pool_name

Specifies the name of the non-pool area to configure with this command.
non_pool_name must be an alpha and/or numeric string of 1 to 63 characters.

use-vlr *vlr_name*

Specifies the name of the VLR to be associated with this non-pool area.
vlr_name is the name of VLR and must be an alpha and/or numeric string of 1 to 63 characters.

lac *lac_num*

Specifies the subscribers' location area code to be attached with this non-pool area and specific VLR. This LAC of subscriber is obtained from the radio area indicator (RAI).
Including this keyword with the **no** form of the command enables the operator to remove a specific LAC from the non-pool area configuration.
lac_num is the LAC value and must be an integer value from 1 through 65535.

+

More than one *lac_num*, separated by a space, can be entered within a single command.

Usage

This command can be repeated as necessary to define a total of 32 configured LACs for the combined **non-pool-area** and **pool-area** configurations per Gs service.

Example

Following command configure a non-pool area *starpool1* to use VLR named *starvlr1* for LAC *101* in a Gs service.

```
non-pool-area starpool1 use-vlr starvlr1 lac 101
```

pool-area

This command creates a pool area configuration instance. This command also enters the Pool Area configuration mode to define the set of VLRs to use for a pool area for a set of subscriber location area code (LAC) values in the Gs service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

pool-area *pool_name* **[-noconfirm]**

no pool-area *non_pool_name*

no

Removes the configured pool area from this Gs service.

pool_name

Specifies the name of the pool area to configure with this command for VLR pooling and association of a LAC.
pool_name: Must be an alpha and/or numeric string of 1 to 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create/enter the pool area configuration mode. This mode is used configure the set of VLRs to be used for a set of subscriber LAC.
This command can be used multiple times, subject to a limit of 128 LAC values (the total number of **non-pool-area** and **pool-area** configurations) per Gs service.

Example

The following command configures a pool area named *starpool1* in a Gs service without any confirmation prompt.

```
pool-area starpool1 -noconfirm
```

sgsn-number

Define the SGSN's E164 number to associate an SGSN with this Gs Service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sgsn-number *E.164_number*

E.164_number

Defines the SGSN's 'telephone' number, the ISDN number for per ITU-T E.164 numbering plan. The number must be a numerical string of 1 to 15 digits.

Usage

For releases 8.1 or higher, use this command to define the SGSN's E.164 ISDN number. This value should match the **sgsn-number** defined for SGSN Service or GPRS Service.

Important: Note: the Gs Service will not start unless the SGSN's E.164 number is configured.

Example

sgsn-number *12345678901234*

timeout

This command configures various timers defining the wait before retransmitting a specific message for Gs service procedures.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

timeout { t6-1-timer *t6_1_dur* **| t8-timer** *t8_dur* **| t9-timer** *t9_dur* **| t10-timer** *t10_dur* **| t12-1-timer minute** *t12_1_dur* **| t12-2-timer** *t12_2_dur***}**

[default] timeout { t6-1-timer | t8-timer | t9-timer | t10-timer | t12-1-timer | t12-2-timer }

default

Sets the timer value to wait in seconds/minutes to default values. Default values for timers are:

- **t6-1-timer**: 10 seconds
- **t8-timer**: 4 seconds
- **t9-timer**: 4 seconds
- **t10-timer**: 4
- **t12-1-timer**: 54 mins (+ 8 seconds)
- **t12-2-timer**: 4 seconds

t6-1-timer *t6_1_dur*

Default: 10
Specifies the retransmission timer value to guard the location update.
t6_1_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 10 through 90.

t8-timer *t8_dur*

Default: 4
Specifies the retransmission timer value to guard the explicit IMSI detach from the GPRS service procedure.
t8_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 30.

t9-timer *t9_dur*

Default: 4
Specifies the retransmission timer value to guard the explicit IMSI detach from the non-GPRS service procedure.
t9_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 30.

t10-timer *t10_dur*

Default: 4
Specifies the retransmission timer value to guard the implicit IMSI detach from the GPRS service procedure.
t10_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 30.

t12-1-timer minute *t12_1_dur*

Default: 54 minutes (plus 8 seconds for transmission delay)
Specifies the retransmission timer value to control the resetting of SGSN-Reset variable procedure.
t12_1_dur is the waiting duration in minutes before retransmitting reset message for the SGSN Reset variable and must be an integer from 0 through 384.

t12-2-timer *t12_2_dur*

Default: 4
Specifies the retransmission timer value to guard the SGSN reset procedure.
t12_2_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 120.

Usage

Use this command to configure the time, for different procedure timers, to wait before retransmitting a procedure message.
This command can be repeated for each timer to configure multiple timers.

Example

Following command sets the timeout duration of 4 seconds for t8 timer to wait before retransmitting the procedure message to explicitly do the IMSI detach from GPRS service:

```
default timeout t8-timer
```

vlr

This command defines a VLR configuration for use with this Gs service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

vlr *vlr_name* **isdn-number** *E164_num* **[bssap+ ssn** *ssn* **] [point-code** *pt_code* **]**

no vlr *vlr_name*

no

Removes the configured VLR from the Gs service.

vlr_name

Specifies the name of the VLR to configure in this Gs mode with ISDN number.
vlr_name must be an alpha and/or numeric string of 1 to 63 characters.

isdn-number *E164_num*

Specifies the VLR number to configure with this command.
E164_num: The ISDN number for the target VLR. Value must be defined according to the E.164 numbering plan and must be a numeric string of 1 to 15 digits.

bssap+ ssn *ssn*

Specifies the subsystem number to configure with this VLR to use BSSAP+.
ssn: Must be an integer from 1 through 255. Default value is 252.

point-code *pt_code*

Specifies SS7 address of VLR in point code value to this configured VLR name.
pt_code: Must be in SS7 point code dotted-decimal ###.###.### format or decimal ######## format.

Usage

Use this command to define VLR configuration instances to be associated with the Gs service.
A maximum of 32 VLRs can be configured per Gs service.

Example

Following command configures the VLR named *starvlr1* with an ISDN number *12344567*, a subsystem number of *252*, and a point code value of *123.345.567*:

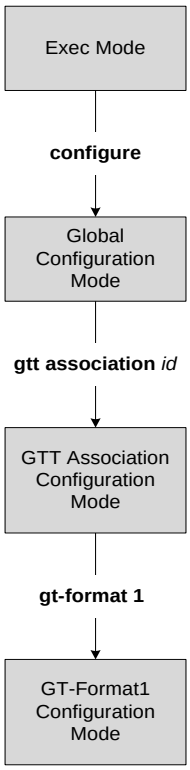
vlr *starvlr1* **isdn-number** *12344567* **point-code** *123.345.567*

Chapter 133
GT-Format1 Configuration Mode Commands

The GT-Format1 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

Upon accessing this mode, your prompt should look similar to the following:

```
[local]<hostname>(config-gtt-1-format1)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the configuration mode and returns to the Global configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the Global configuration mode.

nature-of-address

Configures the indicator to identify the nature of the address.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
nature-of-address { international | national | subscriber )
```

international

Identifies the numbers as international.

national

Identifies the numbers as matching the national configuration.

subscriber

Identifies the numbers as subscriber numbers.

Usage

Configure the identify of the GT format as national.

Example

```
nature-or-address national
```

odd-even-indicator

Configures the bits for matching the global title translation.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

odd-even-indicator *type*

type

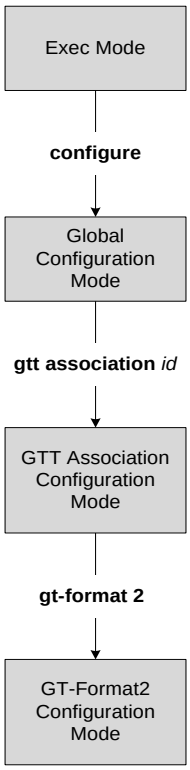
- **odd:** Sets the odd bit for matching the GTT.
- **even:** Sets the even bit for matching the GTT.

Chapter 134
GT-Format2 Configuration Mode Commands

The GT-Format2 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

Upon accessing this mode, your prompt should look similar to the following:

```
[local]<hostname>(config-gtt-format<#>)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the configuration mode and returns to the Global configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Return to the Global configuration mode.

translation-type

Configures the translation type to be applied during the translation process.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

translation-type *number*

number

Must be an integer between 0 and 255.
Default is 0

Usage

Use this command to configure the GTT translation type to be applied during global title translation process.

Example

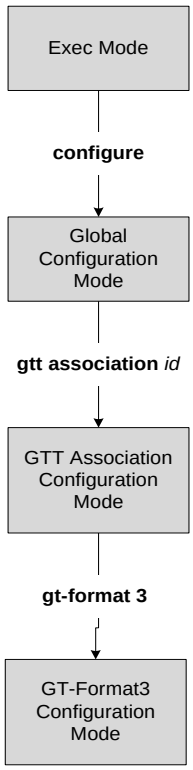
translation-type *232*

Chapter 135
GT-Format3 Configuration Mode Commands

The GT-Format3 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

Upon accessing this mode, your prompt should look similar to the following:

```
[local]<hostname>(config-gtt-1-format<#>)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

encoding-scheme

Configures the encoding-scheme to use during global title translation (GTT).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

encoding scheme *scheme_type*

scheme_type

Select one of the following encoding scheme types to determine the encoding type to be used during GTT:

- **bcd-even:** BCD even encoding scheme
- **bcd-odd:** BCD odd encoding scheme
- **nw-specfic:** Network specific encoding scheme
- **unknown:** Unknown encoding scheme

Usage

Select BCD even encoding for GTT

Example

encoding scheme *bcd-even*

end

Exits the configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the configuration mode and returns to the Global configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the Global configuration mode.

numbering-plan

Configures the GTT process to apply one of the numbering-plans during the GT translation process.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

numbering-plan *plan_type*

plan_type

Select one of the following numbering plans be employed during GTT:

- **data:** Data numbering plan
- **generic**: Generic number plan
- **isdn** : ISDN tel numbering plan
- **isdn-mobile:** ISDN mobile numbering plan
- **land-mobile:** Land mobile numbering plan
- **maritime-mobile:** Maritime mobile numbering plan
- **nw-specific** : Private network / network-specific numbering plan
- **telex:** Telex numbering plan
- **unknown**: Unknown numbering plan

Usage

Select ISN telephone number plan for GTT process.

Example

The following command sets the numbering plan to use during GTT processing to isdn

```
numbering-plan isdn
```

translation-type

Configures the global title translation (GTT) process to apply a specific number for translation during the GTT process.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

translation-type *number*

number

Must be an integer between 0 and 255.
Default is 0

Usage

Use this command to define the translation-type to be used during the global title translation process.

Example

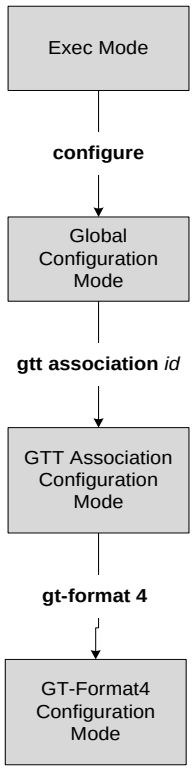
translation-type *233*

Chapter 136
GT-Format4 Configuration Mode Commands

The GT-Format4 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

Upon accessing this mode, your prompt should look similar to the following:

```
[local]<hostname>(config-gtt-1-format<#>)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

encoding-scheme

Configures the encoding-scheme to use during GTT.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

encoding scheme *scheme_type*

scheme_type

Select one of the following encoding scheme types to determine the encoding type to be used during GTT:

- **bcd-even:** BCD even encoding scheme
- **bcd-odd:** BCD odd encoding scheme
- **nw-specfic:** Network-specific encoding scheme
- **unknown:** Unknown encoding scheme

Usage

Select BCD even encoding for GTT

Example

encoding scheme *bcd-even*

end

Exits the configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the configuration mode and returns to the Global configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the Global configuration mode.

nature-of-address

Configures the indicator to identify the nature of the address.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
nature-of-address { international | national | subscriber )
```

international

Identifies the numbers as international.

national

Identifies the numbers as matching the national configuration.

subscriber

Identifies the numbers as subscriber numbers.

Usage

Configure the identify of the GT format as national.

Example

```
nature-or-address national
```

numbering-plan

Configures the GTT process to apply one of the numbering-plans during the GT translation process.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

numbering-plan *plan_type*

plan_type

Select one of the following numbering plans be employed during GTT:

- **data:** Data numbering plan
- **generic**: Generic number plan
- **isdn** : ISDN tel numbering plan
- **isdn-mobile:** ISDN mobile numbering plan
- **land-mobile:** Land mobile numbering plan
- **maritime-mobile:** Maritime mobile numbering plan
- **nw-specific** : Private network/ network-specific numbering plan
- **telex:** Telex numbering plan
- **unknown**: Unknown numbering plan

Usage

Select ISN telephone number plan for GTT process.

Example

numbering-plan *isdn*

translation-type

Configures the GTT process to apply a specific number for translation during the GTT process.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

translation-type *number*

number

Must be an integer between 0 and 255.
Default is 0.

Usage

Use this command to configure the translation-type to be implemented during the global title translation process.

Example

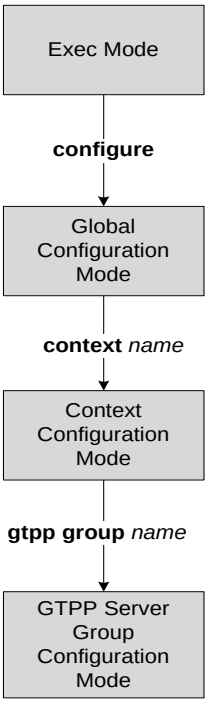
translation-type *231*

Chapter 137
GTPP Server Group Configuration Mode Commands

The GTPP Server Group Configuration Mode is used to create and manage the GTPP server groups within the context or system.

GTPP server group commands facilitate the setup of the hard disk for CDR storage. They also support accounting and charging functionality within a context, and configuration of a group (list) of charging gateway function (CGF) servers on a per subscriber or per GGSN/P-GW APN level.

In this mode, your prompt will be similar to `[context_name]hostname(config-gtpp-group)#`



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

gtpp attribute

Enables the specification of some of the optional fields in the CDRs that the GSN (GGSN or SGSN) generates and/or how the information is to be presented.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp attribute { camel-info | cell-plmn-id | diagnostics | duration-ms | imei | local-record-sequence-number | msisdn | node-id-suffix STRING | plmn-id | rat | record-extensions rat | served-pdp-pdn-address-extension | sms { destination-number | recording-entity | service-centre }  } +

default gtpp attribute { cell-plmn-id | diagnostics | duration-ms | imei | local-record-sequence-number | msisdn | plmn-id | rat | record-extensions rat | served-pdp-pdn-address-extension | sms { destination-number | recording-entity | service-centre } }

no gtpp attribute { cell-plmn-id | diagnostics | duration-ms | imei | local-record-sequence-number | msisdn | node-id-suffix | plmn-id | rat | record-extensions rat | served-pdp-pdn-address-extension | sms { destination-number | recording-entity | service-centre } }
```

default

Resets the default attribute values for this GTPP group configuration.

no

Disables the specified optional field so that the information will not be present in generated CDRs.

camel-info

SGSN only
Enter this keyword to include CAMEL-specific fields in SGSN CDRs. Default: Disabled

cell-plmn-id

SGSN only
Enter this keyword to enable the system to include the Cell PLMN ID field in the M-CDR. Default: Disabled

diagnostics

Default: Disabled
Enables the system to include the Diagnostic field in the CDR that is created when PDP contexts are released. The field will include one of the following values:

- **26** - For GGSN: if the GGSN sends “delete PDP context request” for any other reason (e.g., the operator types “clear subscribers” on the GGSN). For SGSN: The SGSN includes this cause code in the S-CDR to indicate that a secondary PDP context activation request or a PDP context modification request has been rejected due to insufficient resources.

- **36** - For GGSN: this cause code is sent in the G-CDR to indicate the PDP context has been deactivated in the GGSN due to the SGSN having sent a "delete PDP context request" to the GGSN. For SGSN, this cause code is used to indicate a regular MS or network-initiated PDP context deactivation.
- **37** - when the network initiates a QoS modification, the SGSN sends in the S-CDR to indicate that the MS initiation deactivate request message has been rejected with QoS not accepted as the cause.
- **38** - if the GGSN sends "delete PDP context request" due to GTP-C/GTP-U echo timeout with SGSN. If the SGSN sends this cause code, it indicates PDP context has been deactivated due to path failure, specifically GTP-C/GTP-U echo timeout.
- **39** - SGSN only - this code indicates the network (GGSN) has requested a PDP context reactivation after a GGSN restart.
- **40** - if the GGSN sends "delete PDP context request" due to receiving a RADIUS Disconnect-Request message.

`duration-ms`

Specifies that the information contained in the mandatory Duration field be reported in milliseconds instead of seconds (as the standards require). Default: Disabled

`imei`

Default: Disabled
For SGSN: includes the IMEI value in the S-CDR.
For GGSN: includes the IMEISV value in the G-CDR.

`local-record-sequence-number`

Default: Disabled
This keyword provides both the local record sequence number and the Node ID. In the x-CDRs, this field indicates the number of CDRs generated by the node and is unique within the session manager.
The Node ID field is included in the x-CDR for any of several reasons, such as when PDP contexts are released or if partial-CDR is generated based on configuration. The field will consist of a AAA Manager identifier automatically appended to the name of the SGSN or GGSN service.
The name of the SGSN or GGSN service may be truncated, because the maximum length of the Node ID field is 20 bytes. Since each AAA Manager generates CDRs independently, this allows the Local Record Sequence Number and Node ID fields to uniquely identify a CDR.

Important: If this keyword is enabled and the **gtpp centralized-lrsn-creation** option is enabled with the **gtpp single-source centralized-lrsn** command, then the Node ID format changes as follows: <1-byte-AAAproxy-restart-counter> <3-byte AAAproxy instance number> <node-id-suffix>. If **gtpp centralized-lrsn-creation** is not enabled, the node-id format for CDRs generated by Sessmgr is as follows: <1-byte Sessmgr restart-value> <3-byte Sessmgr instance number> <node-id-suffix>. If **gtpp centralized-lrsn-creation** is not enabled, the node-id format for CDRs generated by ACSMGR is as follows: <1-byte ACSmgr restart-value> <3-byte ACSmgr instance number> <Active charging service-name>.

`msisdn`

Default: Enabled
For SGSN: includes the MSISDN value in the S-CDR.
For GGSN: includes the MSISDN value in the G-CDR.

node-id-suffix *STRING*

Default: Disabled
Specifies the configured Node-ID-Suffix to use in the NodeID field of GTPP CDRs as an alphanumeric string of 1 through 16 characters. Each Session Manager task generates a unique NodeID string per GTPP context.

Important: The NodeID field is a printable string of the *ndddSTRING* format: *n*: The first digit is the Sessmgr restart counter having a value between 0 and 7. *ddd*: The number of sessmgr instances. Uses the specified NodeID-suffix in all CDRs. The "Node-ID" field consists of sessMgr Recovery counter (1 digit) *n* + AAA Manager identifier (3 digits) *ddd* + the configured Node-Id-suffix (1 to 16 characters) *STRING*. If the centralized LRSN feature is enabled, the "Node-ID" field will consist of only the specified NodeID-suffix (NodeID-prefix is not included). If this option is not configured, then GTPP group name will be used instead (For default GTPP groups, context-name will be used).

Important: If this **node-id-suffix** is not configured, the GGSN uses the GTPP context name as the Node-id-suffix (truncated to 16 characters) and the SGSN uses the GTPP group named as the node-id-suffix.

plmn-id [unknown-use]

Default: Enabled
For SGSN, reports the SGSN PLMN Identifier value (the RAI) in the S-CDR provided if the dictionary supports it.
For GGSN, reports the SGSN PLMN Identifier value (the RAI) in the G-CDR if it was originally provided by the SGSN in the GTP create PDP context request. It is omitted if the SGSN does not supply one.
Normally when SGSN PLMN-id information is not available, the attribute sgsnPLMNIdentifier is not included in the CDR. This keyword enables the inclusion of the sgsnPLMNIdentifier with a specific value when the SGSN PLMN-id is not available.
unknown-use *hex_num*: is aa hexadecimal number from 0x0 through 0xFFFFFF that identifies a foreign SGSN that has not provided a PLMN-id. For GGSN only.

rat

Default: Enabled
For SGSN: includes the RAT (identifies the radio access technology type) value in the S-CDR.
For GGSN: includes the RAT (identifies the radio access technology type) value in the G-CDR.

record-extensions rat

Default: Disabled
Enables network operators and/or manufacturers to add their own recommended extensions to the CDRs according to the standard record definitions from 3GPP TS 32.298 Release 7 or higher.

served-pdp-pdn-address-extension

Default: Disabled
In support of IPv4v6 dual PDP address types, this keyword causes the SGSN to include IPv4v6 address information in the S-CDR. The IPv4 address goes in the a new PDP address extension field and the IPv6 address goes in the existing servedPDPAdress field.
This keyword is applicable for SGSN only.

sms { destination-number | recording-entity | service-centre }

This keyword is specific to the SGSN.
Entering this keyword causes the inclusion of an SMS-related field in the SMS-MO-CDR or SMS-MT-CDR.

destination-number: Includes the "destinationNumber" field in the SMS-MO-CDR or SMS-MT-CDR.
recording-entity: Includes the "recordingEntity" field in the SMS-MO-CDR or SMS-MT-CDR.
service-centre: Includes the "serviceCentre" field in the SMS-MO-CDR or SMS-MT-CDR.

+

Indicates that this command can be entered multiple times to configure multiple attributes.

Usage

This command dictates some of the optional information fields that should be reported in CDRs generated by the GGSN. In addition, it controls how the information for some of the mandatory fields are reported. Fields described as optional by the standards but not listed above will always be present in the CDRs, except for Record Extensions (which will never be present).

Example

The following command dictates that the time provided in the Duration field of the CDR is reported in milliseconds:

```
gtpp attribute duration-ms
```

gtpp charging-agent

Configures the IP address and port of the system interface within the current context used to communicate with the CGF or the GSS.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp charging-agent address ip_address [ port port ]

no gtpp charging-agent
```

no

Removes a previously configured charging agent address.

address *ip_address*

Specifies the IP address of the interface configured within the current context that is used to transmit G-CDR records to the CGF or the GSS.
ip_address is expressed in IPv4 dotted-decimal notation.

port *port*

Specifies the Charging Agent UDP port as an integer from 1 through 65535. If the port is not defined, the default port number 49999 will be used.

Important: Configuring GTPP charging-agent on port 3386 may interfere with ggsn-service configured with the same ip address.

Usage

This command can be used to establish a UDP interface to connect to the GSS or this command can establish a Ga interface to connect to the CFG. These interfaces must exist in the same context in which GTPP functionality is configured (refer to the **gtpp** commands in this chapter).
This command instructs the system as to what interface to use. The IP address supplied is also the address by which the GGSN/SGSN is known to the CGF or the GSS. Therefore, the IP address used for the Ga or UDP interface could be identical to one bound to a GGSN/SGSN service (a Gn interface).
If no GGSN/SGSN services are configured in the same context as the Ga/UDP interface, the address configured by this command is used to receive unsolicited GTPP packets.

Example

The following command configures the system to use the interface with an IP address of 192.168.13.10 as the accounting interface with port *20000* to the CGF:

```
gtpp charging-agent address 192.168.13.10

gtpp charging-agent address 192.168.13.10 port 20000
```

gtpp data-request sequence-numbers

Configures the range of sequence numbers to be used in the GTPP data record transfer record (DRT). Use this command to set the start value for the sequence number.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp data-request sequence-numbers start { 0 | 1 }

default gtpp data-request sequence-numbers start
```

default

Default is 0 (zero).

start { 0 | 1 }

Specifies the value of the start sequence number for the GTPP Data Record Transfer Request. Default: 0

- **0**: Designates the start sequence number as 0.
- **1**: Designates the start sequence number as 1.

Usage

When the GGSN/P-GW/SGSN is configured to send GTPP echo request packets, the SGSN always uses 0 as the sequence number in those packets. Re-using 0 as a sequence number in the DRT packets is allowed by the 3GPP standards; however, this CLI command ensures the possibility of inter-operating with CGFs that can not properly handle the re-use of sequence number 0 in the echo request packets.

Example

The following command sets the sequence to start at 1.

```
gtpp data-request sequence-numbers start 1
```

gtpp deadtime

Configures the amount of time the GGSN/SGSN waits before attempting to communicate with a CGF that was previously marked as unreachable (non-responsive).

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp deadtime *time*

default deadtime

default

Resets the deadtime to the default of 120 seconds.

time

Specifies the amount of time (in seconds) that must elapse before the system attempts to communicate with a CGF that was previously unreachable.
time is an integer from 1 to 65535. Default: 120

Usage

If the system is unable to communicate with a configured CGF, after a pre-configured number of failures the system marks the CGF as being down.
This command specifies the amount of time that the system waits prior to attempting to communicate with the downed CGF.
Refer to the **gtpp detect-dead-server** and **gtpp max-retries** commands for additional information on the process the system uses to mark a CGF as down.

Example

The following command configures the system to wait 60 seconds before attempting to re-communicate with a CGF that was marked as down:

```
gtpp deadtime 60
```

gtpp dead-server suppress-cdrs

Configures the action the GGSN or the SGSN will take on CDRs generated during a communication failure between the GGSN or the SGSN and the GTPP servers.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] gtpp dead-server suppress-cdrs
```

no

Removes the suppression instruction from the configuration and sets the CDR suppression mode as disabled.

default

Resets the GGSN or the SGSN to the default mode: disable suppression of CDRs when GTPP server detected as “dead” or unreachable.

Usage

For the GGSN/P-GW: This command works in conjunction with the **gtpp detect-dead-server** to set an action when a communication failure is detected between the GGSN and a configured GTPP server. It disables the archiving of CDRs on the system when the GTPP server is unreachable or dead.
For the GGSN. P-GW, and the SGSN: During a communication or server failure, the GGSN, P-GW, or SGSN typically retains the GTPP requests until the system buffer runs out of resources. This command enables suppression of the CDRs, so with this command the GGSN, P-GW, or the SGSN will start purging all CDRs associated with this GTPP group as soon as the GGSN/P-GW/SGSN detects that the GTPP server is down or that a communication failure has occurred. The CDRs generated, for the period while the server is down/unreachable, will also be purged.

Example

The following command configures the system to start purging CDRs when a communication failure with a server is detected:

```
gtpp dead-server suppress-cdrs
```

gtpp detect-dead-server

Configures the number of consecutive communication failures that could occur before the system marks a CGF as "dead" (unreachable).

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp detect-dead-server consecutive-failures *max_number*

default gtpp detect-dead-server consecutive-failures

default

Resets the system to the default number of consecutive failures.

consecutive-failures *max_number*

Default: 5
Specifies the number of failures that could occur before marking a CGF as down as an integer from 0 through 1000. If 0 (zero) is the value entered, the system will mark the CGF as dead after a single instance of **max-retries** has been attempted with no success, regardless of configured **deadtime**.

Usage

This command works in conjunction with the **gtpp max-retries** parameter to set a limit to the number of communication failures that can occur with a configured CGF.
The **gtpp max-retries** parameter limits the number of attempts to communicate with a CGF. Once that limit is reached, the system treats it as a single failure. The **gtpp detect-dead-server** parameter limits the number of consecutive failures that can occur before the system marks the CGF as down and communicate with the CGF of next highest priority.
If all of the configured CGFs are down, the system ignores the detect-dead-server configuration and attempt to communicate with highest priority CGF again.
If the system receives a GTPP Node Alive Request, Echo Request, or Echo Response message from a CGF that was previously marked as down, the system immediately treats it as being active.
Refer to the **gtpp max-retries** command for additional information.

Example

The following command configures the system to allow 8 consecutive communication failures with a CGF before it marks it as down:

```
gtpp detect-dead-server consecutive-failures 8
```

gtpp dictionary

Designates specific dictionary used by GTPP for specific context.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp dictionary { **custom1** | **custom10** | **custom11** | **custom12** | **custom13** | **custom14** | **custom15** | **custom16** | **custom17** | **custom18** | **custom19** | **custom2** | **custom20** | **custom21** | **custom22** | **custom23** | **custom24** | **custom25** | **custom26** | **custom27** | **custom28** | **custom29** | **custom3** | **custom30** | **custom31** | **custom32** | **custom33** | **custom34** | **custom35** | **custom36** | **custom37** | **custom38** | **custom39** | **custom4** | **custom40** | **custom41** | **custom42** | **custom43** | **custom44** | **custom45** | **custom46** | **custom47** | **custom48** | **custom49** | **custom5** | **custom50** | **custom51** | **custom52** | **custom53** | **custom54** | **custom55** | **custom56** | **custom57** | **custom58** | **custom59** | **custom6** | **custom60** | **custom7** | **custom8** | **custom9** | **standard** }**default gtpp dictionary**

default gtpp dictionary

---

default

Configures the default dictionary.

---

custom1

Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99. It supports the encoding of IP addresses in text format for G-CDRs.

---

custom2

Custom-defined dictionary.

---

custom3

Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99 but it does support the encoding of IP addresses in binary format for CDRs.

---

custom4

Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99 except that:

- the Data Record Format Version information element contains 0x1307 instead of 0x1308
- "QoSRequested" is not present in the LoTV containers
- "QoSnegotiated" is added only for the first container and the container after a QoS change

---

custom5 ... custom20

Custom-defined dictionaries.

custom21 ... custom25

Custom-defined dictionaries for GGSN only.

custom26

Custom-defined dictionary for customization of G-CDR records for GGSN only. This is compliant to 3GPP TS 32.298 (R6 v 6.5.0) for proprietary fields and encoding.

custom27

Custom-defined dictionary for customization of S-CDR records for SGSN only. This is compliant to 3GPP TS 32.298 (R6 v 6.6.0) for proprietary fields and encoding.

custom28 ... custom30

Custom-defined dictionaries for GGSN only.

custom31 ... custom40

Custom-defined dictionaries based on 3GPP 32.298 v6.4.1 for SGSN only.

- **custom31:** Custom-defined dictionary for S-CDR encoding. Includes a field appended for PLMN-ID.
- **custom33:** Custom-defined dictionary for S-CDR encoding. Includes a field appended for PLMN-ID and does not support diagnostic or SGSN-change fields.

standard

Default: Enabled
A dictionary conforming to TS 32.215 v 4.6.0 for R4 (and also R5 - extended QoS format).

Usage

Use this command to designate specific dictionary used by GTPP for specific context.

Example

The following command configures the system to use custom3 dictionary to encode IP address in Binary format in G-CDRs:

```
gtpp dictionary custom3
```

gtpp duplicate-hold-time

Configures the number of minutes to hold onto CDRs that are possibly duplicates while waiting for the primary CGF to come back up.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp duplicate-hold-time minutes *minutes*

default gtpp duplicate-hold-time

default

Resets the configuration to the default value of 60 minutes for the duplicate hold time.

minutes

When the primary CGF is down, the number of minutes to hold onto CDRs that may be duplicates. *minutes* must be an integer from 1 to 10080. Default is 60.

Usage

Use this command to configure how long to hold onto CDRs, that are possibly duplicates, while waiting for the primary CGF to come back up. If the GGSN determines that the primary CGF is down, CDRs that were sent to the primary CGF, but not acknowledged, are sent by the GGSN to the secondary CGF as "possibly duplicates". When the primary CGF comes back up, the GGSN uses GTPP to determine whether the possibly duplicate CDRs were received by the primary CGF. Then the secondary CGF is told whether to release or cancel those CDRs. This command configures how long the system should wait for the primary CGF to come back up. As soon as the configured time expires, the secondary CGF is told to release all of the possibly duplicate CDRs.

Example

Use the following command to set the amount of time to hold onto CDRs to 2 hours (120 minutes):

```
gtpp duplicate-hold-time minutes 120
```

gtpp echo-interval

Configures the frequency at which the system sends GTPP echo packets to configured CGFs.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp echo-interval time

{ default | no } gtpp echo-interval
```

default

Resets the configuration to the default echo-interval of 60 seconds.

no

Disables the use of the echo protocol except for the scenarios described in the Usage section for this command.

time

Specifies the number of seconds for sending GTPP echo packets as an integer from 60 to 3600. Default: 60.

Usage

The GTPP echo protocol is used by the system to ensure that it can communicate with configured CGFs. The system initiates this protocol for each of the following scenarios:

- Upon system boot
- Upon the configuration of a new CGF server on the system using the **gtpp server** command as described in this chapter
- Upon the execution of the **gtpp test accounting** command as described in the Exec Mode Commands chapter of this reference
- Upon the execution of the **gtpp sequence-numbers private-extensions** command as described in this chapter

The echo-interval command is used in conjunction with the **gtpp max-retries** and **gtpp timeout** commands as described in this chapter.
In addition to receiving an echo response for this echo protocol, if we receive a GTPP Node Alive Request message or a GTPP Echo Request message from a presumed dead CGF server, we will immediately assume the server is active again.
The alive/dead status of the CGFs is used by the AAA Managers to affect the sending of CDRs to the CGFs. If all CGFs are dead, the AAA Managers will still send CDRs, (refer to the **gtpp deadtime** command), albeit at a slower rate than if a CGF were alive. Also, AAA Managers independently determine if CGFs are alive/dead.

Example

The following command configures an echo interval of 120 seconds:

```
gtpp echo-interval 120
```

gtpp egcdr

Configures the eG-CDR and P-CDR (P-GW CDR) parameters and triggers.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
gtpp egcdr { final-record [ [ include-content-ids { all | only-with-traffic } ] [
closing-cause { same-in-all-partials | unique } ] ] | losdv-max-containers
max_losdv_containers | lotdv-max-containers max_lotdv_containers | rulebase-max-length
rulebase_name_max_length | service-data-flow threshold { interval interval | volume {
downlink bytes [ uplink bytes ] | total bytes | uplink bytes [ downlink bytes ] } } |
service-idle-timeout { 0 | service_idle_timeout } }

default gtpp egcdr { final-record include-content-ids only-with-traffic closing-cause
same-in-all-partials | losdv-max-containers | lotdv-max-containers | service-idle-timeout
0 }

no gtpp egcdr { rulebase-max-length | service-data-flow threshold { interval | volume {
downlink [ uplink ] | total | uplink [ downlink ] } } }
```

final-record [[include-content-ids { all | only-with-traffic }] [closing-cause { same-in-all-partials | unique }]]

Enables configuration of the final eG-CDR/P-CDR.

- **include-content-ids**: Controls which content-ids are being included in the final eG-CDR/P-CDR.
  - **all**: Specifies that all content-ids be included in the final eG-CDR/P-CDR.
  - **only-with-traffic**: Specifies that only content-ids with traffic be included in the final eG-CDR/P-CDRs.
- **closing-cause**: Configures closing cause for the final eG-CDR/P-CDR.
  - **same-in-all-partials**: Specifies that the same closing cause is to be included for multiple final eG-CDR/P-CDRs.
  - **unique**: Specifies that the closing cause for final eG-CDR/P-CDRs is to be unique.

losdv-max-containers *max_losdv_containers*

Specifies the maximum number of List of Service Data Volume (LoSDV) containers in one eG-CDR/P-CDR.
max_losdv_containers must be an integer from 1 through 255.
Default: 10

lotdv-max-containers *max_lotdv_containers*

Specifies the maximum number of List of Traffic Data Volume (LoTDV) containers in one eG-CDR/P-CDR.
max_lotdv_containers must be an integer from 1 through 8.
Default: 8

rulebase-max-length *rulebase_name_max_length*

Specifies the maximum character length of charging rulebase name in LOSDVs of eG- CDR/P-GW-CDR. *rulebase_name_max_length* must be an integer from 0 through 63. Zero (0) means the rulebase name is added as-is.
Default: None. That is, full (un-truncated) charging rulebase name will go in LOSDVs of eG-CDR/P-GW-CDR.

service-data-flow threshold { interval *interval* **| volume { downlink** *bytes* **[uplink** *bytes* **] | total** *bytes* **| uplink** *bytes* **[downlink** *bytes* **] } }**

Configures the thresholds for closing a service data flow container within an eG-CDR/P-CDR.

- **interval** *interval*: Specifies the time interval (in seconds) to close the eG-CDR/P-CDR if the minimum time duration thresholds for service data flow containers satisfied in flow-based charging. The interval is an integer from 60 through 40000000. Default: Disabled
- **volume { downlink** *bytes* **[uplink** *bytes* **] | total** *bytes* **| uplink** *bytes* **[downlink** *bytes* **] }**: Specifies the volume octet counts for the generation of the interim eG-CDR/P-CDRs to the service data flow container in FBC.
  - **downlink** *bytes*: Specifies the limit for the number of downlink octets after which the eG-CDR/P-CDR is closed.
  - **total** *bytes*: Specifies the limit for the total number of octets (uplink+downlink) after which the eG-CDR/P-CDR is closed.
  - **uplink** *bytes*: Specifies the limit for the number of uplink octets after which the eG-CDR/P-CDR is closed.
  - *bytes* must be an integer from 10000 through 400000000.

A service data flow container has statistics for an individual content ID. When the threshold is reached, the service data flow container is closed.

service-idle-timeout { 0 | *service_idle_timeout***}**

Specifies a time period during which if no data is reported for a service flow, the service container is closed and added to eG-CDR/P-CDR (as part of LOSDV container list) with service condition change as ServiceIdleOut.
0: Specifies there is no service-idle-timeout trigger.
service_idle_timeout is an integer from 10 through 86,400. Default: 0

Usage

Use this command to configure individual triggers for eG-CDR/P-CDR generation.

Example

Use the following command to set the maximum number of LoSDV containers to 7:

```
gtpp egcdr losdv-max-containers 7
```

gtpp error-response

Configures the response when the system receives an error response after transmitting a DRT (data record transfer) request.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp error-response { discard-cdr | retry-request }

default gtpp error-response
```

default

Resets the system's configuration to the default value for error-response. Default is retry-request.

discard-cdr

Purges the request upon receipt of an error response and not to retry.

retry-request

Retries sending a DRT after receiving an error response. This is the default behavior.

Usage

This command configures the system's response to receiving an error message after sending a DRT request.

Example

```
gtpp error-response discard-cdr
```

gtpp max-cdrs

Configures the maximum number of charging data records (CDRs) to be included in a packet.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp max-cdrs *max_cdrs* **[wait-time** *wait_time* **]**

default gtpp max-cdrs

default

Sets the default configuration.

max_cdrs

Specifies the maximum number of CDRs to insert in a single packet as an integer from 1 through 255.
Default: 1

wait-time*wait_time*

Specifies the number of seconds the GSN waits to send the packet while accumulating CDRs as defined by **max-cdrs**. If the **wait-time** interval expires before **max-cdrs** is reached, this keyword over-rides and the packet is sent. Default: Disabled
wait_time is an integer from 1 through 300.

Important: The **wait-time** interval can only be enabled if the value for **max-cdrs** is greater than 1.

Usage

The system places CDRs into a packet until either **max-cdrs** is met, **wait-time** times out, or the maximum PDU size, configured by the **gtpp max-pdu-size** command, is met.
The **gtpp max-pdu-size** and the **wait-time** parameters take priority over **max-cdrs**.

Important: This command's configuration is ignored if CDRs are stored on an SMC hard disk.

Example

The following command configures the system to place a maximum of 10 CDRs in a single GTPP packet with a wait-time of *30* seconds:

```
gtpp max-cdrs 10 wait-time 30
```

gtpp max-pdu-size

Configures the maximum payload size of a single GTPP packet that could be sent by the system.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp max-pdu-size *pdu_size*

default gtpp max-pdu-size

default

Resets the default **max-pdu-size** of 4096.

pdu_size

Specifies the maximum payload size (in bytes) of the GTPP packet as an integer from 1024 to 65400. The payload includes the CDR and the GTPP header. Default: 4096

Usage

The GTPP packet contains headers (layer 2, IP, UDP, and GTPP) followed by the CDR. Each CDR contains one or more volume containers. If a packet containing one CDR exceeds the configured maximum payload size, the system creates and send the packet containing the one CDR regardless.
The larger the packet data unit (PDU) size allowed, the more volume containers that can be fit into the CDR. The system performs standard IP fragmentation for packets that exceed the system's maximum transmission unit (MTU).

Important: The maximum size of an IPv4 PDU (including the IPv4 and subsequent headers) is 65,535. However, a slightly smaller limit is imposed by this command because the system's max-pdu-size doesn't include the IPv4 and UDP headers, and because the system may need to encapsulate GTPP packets in a different/larger IP packet (for sending to a backup device).

Example

The following command configures a maximum PDU size of 2048 octets:

```
gtpp max-pdu-size 2048
```

gtpp max-retries

Configures the maximum number of times the system attempts to communicate with an unresponsive CGF.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp max-retries *max_attempts*

default gtpp max-retries

default

Resets the maximum number of to the default of 4.

max_attempts

Specifies the number of times the system attempts to communicate with a CGF that is not responding as an integer from 1 to 15. Default: 4

Usage

This command works in conjunction with the **gtpp detect-dead-server** and **gtpp timeout** parameters to set a limit to the number of communication failures that can occur with a configured CGF.
When the value specified by this parameter is met, a failure is logged. The **gtpp detect-dead-server** parameter specifies the number of consecutive failures that could occur before the server is marked as down. In addition, the **gtpp timeout** command controls the amount of time between re-tries.
If the value for the max-retries is met, the system begins storing CDRs in Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context). Archived CDRs are re-transmitted to the CGF until they are acknowledged or the system's memory buffer is exceeded.
Refer to the **gtpp detect-dead-server** and **gtpp timeout** commands for additional information.

Example

The following command configures the maximum number of re-tries to be 8.

```
gtpp max-retries 8
```

gtpp mbms bucket

Configures the traffic data volume (bucket) limit of charging buckets due to QoS changes of tariff time that can occur before a G-MBMS-CDR should be closed.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp mbms buckets *number*

[no] gtpp mbms buckets

no

Disables the configured traffic data volume bucket limits trigger for G-MBMS-CDR generation for MBMs user service data.

buckets *number*

Specifies the number of statistics container changes due to QoS changes or tariff time that can occur before a G-MBMS-CDR should be closed as an integer from 1 through 4. Default: 4

Usage

Use this command to configure the traffic data volume (bucket) based G-MBMS-CDR generation triggers for MBMS user data service.

Example

The following command configures the bucket-based trigger to generate G-MBMS-CDRs after changes in *2* container:

```
gtpp mbms buckets 2
```

gtpp mbms interval

Configures the interval duration for interval-based triggers for GTPP MBMS Charging Data Record (G-MBMS-CDR) generation.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp mbms interval *duration_sec*

no gtpp mbms interval

no

Disables the interval-based trigger for G-MBMS-CDR generation for MBMs user service data.

interval *duration_sec*

Specifies the normal time duration (in seconds) that must elapse before closing an accounting record provided that any or all of the following conditions occur:

- Downlink traffic volume is reached within the time interval
- Tariff time based trigger occurred within the time interval
- Data volume (up and downlink) bucket trigger occurred within the time interval

duration_sec is an integer from 60 through 40,000,000. Default: Disabled

Usage

Use this command to configure the G-MBMS-CDR generation triggers for MBMS user data service.

Example

The following command configures the interval-based trigger to generate G-MBMS-CDRs in every *60* seconds:

```
gtpp mbms interval 60
```

gtpp mbms tariff

Configures the tariff slots for tariff-based triggers for GTPP MBMS Charging Data Record (G-MBMS-CDR) generation.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp mbms tariff time1 *mins hours* **[time2** *mins hours* **[time3***mins hours* **[time4***mins hours* **]]]**

[no] gtpp mbms tariff

no

Disables the tariff-based triggers for GTPP MBMS Charging Data Record (G-MBMS-CDR) generation.

tariff time1 *mins hours* **[time2***mins hours* **[time3***mins hours* **[time4***mins hours* **]]]**

Specifies time-of-day time values to close the current statistics container (but not necessarily the accounting record). Default: Disabled

Important: The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

For each of the different tariff times, the following parameters must be configured:

- *mins*: Minute of the hour, an integer from 0 through 59.
- *hours*: Hour of the day, an integer from 0 through 23.

Usage

Use this command to configure the tariff-time-based triggers for G-MBMS-CDR generation in MBMS user data service.

Example

The following command configures the tariff-time-based trigger to generate G-MBMS-CDRs every day at 11 hours and 30 min:

```
gtpp mbms tariff time1 30 11
```

gtpp mbms volume

Configures the download traffic data volume based trigger for GTPP MBMS Charging Data Record (G-MBMS-CDR) generation.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp mbms volume *download_bytes*

[no] gtpp mbms volume

no

Disables the configured download traffic data volume based trigger for G-MBMS-CDR generation for MBMs user service data.

volume *download_bytes*

Specifies the threshold of downlink data volumes that (in bytes) must be met before a G-MBMS-CDR should be closed as an integer from 100000 through 4000000000. Default: Disabled

Usage

Use this command to configure the traffic data volume (download) based G-MBMS-CDR generation triggers for MBMS user data service.

Example

The following command configures the traffic data volume (download) limit to trigger to generate G-MBMS-CDRs after reaching 150,000 octets:

```
gtpp mbms volume download_bytes
```

gtpp redirection-allowed

Configures the system to allow/disallow the redirection of CDRs when the primary CGF is unavailable.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] gtpp redirection-allowed
```

default

Resets the system to allow redirection of CDRs.

no

Removes the redirection definition from the configuration.

Usage

This command allows operators to better handle erratic network links, without having to remove the configuration of the backup server(s) via the **no gtpp server** command.
This functionality is enabled by default.
If the **no gtpp redirection-allowed** command is executed, the system only sends CDRs to the primary CGF. If that CGF goes down, the system will buffer the CDRs in memory until the CGF comes back or until the system runs out of buffer memory. In addition, if the primary CGF announces its intent to go down (with a GTPP Redirection Request message), the system responds to that request with an error response.

Example

The following command configures the system to allow the redirection of CDRs when the primary CGF is unavailable:

```
default gtpp redirection-allowed
```

gtpp redirection-disallowed

This command has been obsoleted and is replaced by the **gtpp redirection-allowed** command.

gtpp server

Configures the charging gateway function (CGF) accounting server(s) with in GTPP server group that the system is to communicate with.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp server *ip_address* **[max** *msgs* **] [priority** *priority* **] [udp-port** *port* **] [node-alive { enable | disable }] [-noconfirm]**

no gtpp server *ip_address* **[udp-port** *port* **]**

no

Deletes a previously configured CGF.

ip_address

Specifies the IP address of the CGF in IPv4 dotted-decimal or IPv6 colon-separated notation.

max *msgs*

Specifies the maximum number of outstanding or unacknowledged GTPP packets (from any one AAA Manager task) allowed for this CGF before the system begins buffering the packets.
msgs can be configured to an integer from 1 to 256. Default: 256

priority*priority*

Default:1000
Specifies the relative priority of this CGF as an integer from 1 through 1000. When multiple CGFs are configured, the priority is used to determine which CGF server to send accounting data to. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this.
If you use the **-noconfirm** option, you are not asked for confirmation and multiple servers could be assigned the same priority.

udp-port*port*

Specifies the UDP port over which the GGSN communicates with the CGF. as an integer from 1 through 65535. Default: 3386

node-alive { enable | disable }

Enable or disables GGSN sending Node Alive Request to a GTPP Server (such as CGF). This configuration can be done per GTPP Server. Default: Disable.

-noconfirm

Executes this command without any additional prompt and confirmation from the user.

Usage

Use this command to configure the CGF(s) that the system sends CDR accounting data to.
Multiple CGFs can be configured using multiple instances of this command subject to the following limits:

- Up to 4 CGFs can be configured in one GTPP server group
- Total of 32 CGFs can be configured per context.

Each configured CGF can be assigned a priority. The priority is used to determine which server to use for any given subscriber based on the routing algorithm that has been implemented. A CGF with a priority of "1" has the highest priority.

Important: The configuration of multiple CGFs with the same IP address but different port numbers is not supported.

Each CGF can also be configured with the maximum allowable number of unacknowledged GTPP packets. Since multiple AAA Manager tasks could be communicating with the same CGF, the maximum is based on any one AAA Manager instance. If the maximum is reached, the system buffers the packets Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context).

Example

The following command configures a CGF with an IP address of 192.168.2.2 and a priority of 5.

```
gtpp server 192.168.2.2 priority 5
```

The following command deletes a previously configured CGF with an IP address of 100.10.35.7:

```
no gtpp server 100.10.35.7
```

gtpp source-port-validation

Configures whether the system validates the UDP source port in received GTPP messages.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[no | default] gtpp source-port-validation
```

no

Validates the IP source address but not the UDP source port.

default

Restores this parameter to its default setting of enabled.

Usage

This command configures whether the system validates the UDP source port in received GTPP messages.

Example

The following command disables UDP port validation:

```
no gtpp source-port-validation
```

gtpp storage-server

Configures information for the GTPP back-up storage server.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] gtpp storage-server *ip_address* **port** *port_num*

no

Removes a previously configured back-up storage server.

ip_address

The IP address of the back-up storage server expressed in IPv4 dotted-decimal notation.

port *port_num*

Specifies the UDP port number over which the GGSN communicates with the back-up storage server.
Default: 3386

Usage

This command identifies the connection to the GSS. One backup storage server can be configured per GTPP group.

Example

The following command configures a GSS with an IP address of 192.168.1.2:

```
gtpp storage-server 192.168.1.2
```

gtpp storage-server local file

Configures the parameters for GTPP files stored locally on the GTPP storage server.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpp storage-server local file { **compression** { **gzip** | **none** } | **format** { **custom1** | **custom2** | **custom3** | **custom4** | **custom5** | **custom6** | **custom7** | **custom8** } | **name** { **format** *string* [**max-file-seq-num** *seq_number*] | **prefix** *prefix* } | **purge-processed-files** [**file-name-pattern** *name_pattern* | **purge-interval** *purge_interval*] | **rotation** { **cdr-count** *count* | **time-interval** *time* [**force-file-rotation**] | **volume mb** *size* } | **start-file-seq-num** *seq_num* [**recover-file-seq-num** }

default gtpp storage-server local file { **compression** | **format** | **name** { **format** | **prefix** } | **purge-processed-files** | **rotation** { **cdr-count** | **time-interval** | **volume** } **start-file-seq-num** }

no gtpp storage-server local file { **purge-processed-files** | **rotation** { **cdr-count** | **time-interval** } }

---

no

Removes a previously configured parameters for local storage of CDR files on HDD on SMC card.

---

compression { gzip | none }

Configures the type of compression to be used on the files stored locally.
gzip – Enables Gzip file compression.
none – Disables Gzip file compression -this is the default value.

---

format custom1 .. 8

Configures the file format to be used to format files to be stored locally.
custom1 – File format custom1 - this is the default file format.
custom2 to custom5 Customer specific CDR file formats.
custom6 – File format custom6 with a block size of 8K for CDR files.
custom7 – File format custom7 is a customer specific CDR file format.
custom8 – File format custom8 is a customer specific CDR file format. It uses *node-id-suffix_date_time_fixed-length-seq-num*.u format for file naming where:

- *date* is date in MMDDYYYYY (01312010) for mat
- *time* is time in HHMMSS (023508) format
- *fixed-length-seq-num* is the fixed length of the sequence number for s specific file having a 6-digit counter starting from 000001 and ending at 999999. When file sequence reaches 999999, the sequence is reset to 000001.

name format *string*

Allows the format of the CDR filenames to be configured independently so that the name format contains the file name with conversion specifications.
string –is an alphanumeric string of 1 through 127 characters. It **must begin** with the % (percent sign).

- **%y** = year as a decimal number without century (range 00 to 99).
- **%Y** = year as a decimal number with century.
- **%m** = month as a decimal number (range 01 to 12).
- **%d** = day of the month as a decimal number (range 01 to 31).
- **%H** = hour as a decimal number 24-hour format (range 00 to 23).
- **%h** = hour as a decimal number 12-hour format (range 01 to 12).
- **%M** = minute as a decimal number (range 00 to 59).
- **%S** = second as a decimal number (range 00 to 60). (The range is up to 60 to allow occasional leap seconds.)
- **%Q** = file sequence number. Field width may be specified between the % and the Q. If the natural size of the field is smaller than this width, then the result string is padded (on the left) to the specified width with 0s
- **%N** = No of CDRs in the file. Field width may be specified between the % and the N. If the natural size of the field is smaller than this width, then the result string is padded (on the left) to the specified width with 0s
- **%%** = This field is used to add % to the CDR file name.
- **max-file-seq-no**: This can be configured optionally. It indicates the maximum value of sequence number in file name (starts from 1). Once the configured max-file-seq-no limit is reached, the sequence number will restart from 1. If no max-file-seq-no is specified then file sequence number ranges from 1- 4294967295.

By default the above keyword is not configured (default gtpp storage-server local file name format). In which case the CDR filenames are generated based on the file format as before (maintains backward compatibility).

name prefix *prefix*

Defines the prefix to be used for the file name. By default the file name prefix would be “GTPP-group-name + VPN-ID”. It is possible to have a NULL value prefix where the system would enter a default, which would be *group+vpn*,
prefix – is an alphanumeric string of 1 through 64 characters, Do not enter a value (NULL).

purge-processed-files [file-name-pattern *name_pattern* **| purge-interval** *purge_interval* **]**

Default: Disabled
Enables the GSN to periodically delete locally processed (*.p) CDR files from the HDD on the SMC card.

Important: This option is available only when GTPP server storage mode is configured for local storage of CDRs with the **gtpp storage-server mode local** command and the **purge-processed-files parameters** is enabled.

file-name-pattern *name_pattern*: Defines a pattern for the file name that will be used to match against the files to be purged. This means that the only files to be selected and deleted will be those with

names matching this pattern and whose age (when to purge) has been specified with the existing **purge-interval** parameter.
name_pattern is an alphanumeric string of up to127 characters that can contain '*' (wild card to match 0+ chars) and one or more ':' (to specify alternate, synonymous with '|'); for example: file-name-pattern "*.P:*.dat" matches "anything.P" AND "anything.dat"
purge-interval *purge_interval*: Specifies the purge interval duration in minutes as an integer from 1 through 259200. Default: 60

---

rotation { cdr-count *count* **| time-interval** *time* **[force-rotation] | volume** *size* **}**

Specifies rotation related configuration for GTPP files stored locally.
cdr-count *count*: Configures the CDR count for the file rotation as an integer from 1000 through 65000. Default value 10000.
time-interval *time*: Configures the time interval for file rotation (in seconds) as an integer from 30 through 86400. Default: 3600 (1 hour).
force-file-rotation : Forces CDR file-rotation at a specified interval configured via the **time-interval** keyword, even if no CDRs were generated. By default this keyword is Disabled.
volume *size* **—**: Configures the file volume (in megabytes) for file rotation as an integer from 2 through 40. This trigger can not be disabled. Default: 10

---

start-file-seq-num *seq_num* **[recover-file-seq-num**

Default: disabled
Enables the continuous file sequence number function. **start-file-seq-num** specifies the lowest number to be used as a file sequence number in the case of an aaaproxy or a chassis restart/reboot.
seq_num is an integer from 1 to 4294967295. Entering a value of 1 disables the recover file sequence number function. Entering any other number, for example 10, would instruct the system to always start from 10 as the file sequence number in the event of an aaaproxy or chassis reload.
When files are moved, the file sequence numbers are synced and stored in both RAM and the hard disk drive (HDD). **recover-file-seq-num** instructs the system to recover the last (largest) stored file sequence number, in the event of an aaaproxy/chassis restart/reboot, to continue file sequence numbering rather than resetting the file sequence numbering to the lowest start file sequence number.

Usage

This command configures the parameters for storage of GTPP packets as files on the local server - meaning the hard disk drive (HDD).

Example

The following command configures rotation for every 1.5 hours for locally stored files.

```
gtpp storage-server local file rotation time-interval 5400
```

Configuring file name format along with max-file-seq-no:

```
gtpp storage-server local file name format processed_2g_%Y%m%d_%5Q_%N.cdr
max-file-seq-no 2345
```

Configuring file name prefix with a NULL value:

```
gtpp storage-server local file name prefix NULL
```

Configure the file name pattern and purge interval to setup file purging from the HDD:

```
gtpp storage-server local file purge-processed-files file-name-pattern
*.z purge-interval 4
```

gtpp storage-server max-retries

Configures the maximum number of times the system attempts to communicate with an unresponsive GTPP back-up storage server.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

[default] gtpp storage-server max-retries *max_attempts*

default

Restores the system to the default value of 2 retry attempts.

max_attempts

Specifies the number of times the system attempts to communicate with a GTPP back-up storage server that is not responding as an integer from 1 to 15. Default: 2

Usage

This command works in conjunction with the **gtpp storage-server timeout** parameters to set a limit to the number of communication failures that can occur with a configured GTPP back-up storage server.
The **gtpp storage-server timeout** command controls the amount of time between retries. Refer to the description of this command for additional information.

Example

The following command configures the maximum number of re-tries to be 8.

```
gtpp storage-server max-retries 8
```

gtpp storage-server mode

Configures storage mode, local or remote, for CDRs. Local storage mode is available with ASR 5000 platforms only.

Product

GGSN, P-GW, SGSN, S-GW

Privilege

Security Administrator, Administrator

Syntax

```
gtpp storage-server mode { local | remote | streaming }

default gtpp storage-server mode
```

default

Returns the GTPP group configuration to the default "remote" value for the GTPP storage server mode.

local

Specifies the use of the hard disk for storing CDRs. Default: Disabled

Important: This option is available with ASR 5000 platforms only.

remote

Specifies the use of an external server for storing CDRs. This is the default value.

Important: When the external server is down, the Session Managers will start buffering up to a maximum of 26400 CDRs or a total of 120 MB worth of CDRs, whichever limit reaches first. The maximum CDR limit specified is per the session manager. The chassis level limit varies depending on the number of session manager instances and number of active cards.

streaming

Default: Disabled
This keyword allows the operator to configure "streaming" mode of operation for GTPP group. When this keyword is supplied the CDRs will be stored in following fashion:

- When GTPP link is active with CGF, CDRs are sent to a CGF via GTPP and local hard disk is NOT used as long as every record is acknowledged in time.
- If the GTPP connection is considered to be down, all streaming CDRs will be saved temporarily on the local hard disk and once the connection is restored, unacknowledged records will be retrieved from the hard disk and sent to the CGF.

Important: This option is available with ASR 5000 platforms only.

Usage

This command configures whether the CDRs should be stored on the hard disk of the SMC or remotely, on an external server.

Example

The following command configures use of a hard disk for storing CDRs.

```
gtpp storage-server mode local
```

gtpp storage-server timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the GTPP back-up storage server.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

[default] gtpp storage-server timeout *duration*

default

Restores the timeout duration to the default of 30 seconds.

duration

Specifies the maximum amount of time (in seconds) that the system waits for a response from the GTPP back-up storage server before assuming the packet is lost.
duration is an integer from 30 through 120. Default: 30

Usage

This command works in conjunction with the **gtpp storage-server max-retries** command to establish a limit on the number of times that communication with a GTPP back-up storage server is attempted before a failure is logged.
This parameter specifies the time between retries.

Example

The following command configures a retry timeout of *60* seconds:

```
gtpp storage-server timeout 60
```

gtpp suppress-cdrs zero-volume-and-duration

Suppresses the CDRs created by session having zero duration and/or zero volume. By default this mode is “disabled”.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
gtpp suppress-cdrs zero-volume-and-duration { gcdrs [ egcdrs ] | egcdrs [ gcdrs ] }

default gtpp suppress-cdrs zero-volume-and-duration
```

default

Disables the CDR suppression mode.

gcdrs [egcdrs]

Specifies that this command will handle G-CDRs before eG-CDR/P-CDRs.

gcdrs [egcdrs]

Specifies that this command will handle eG-CDR/P-CDRs before G-CDRs.

Usage

Use this command to suppress the CDRs (G-CDRs and eG-CDR/P-CDRs) which were created due with zero-duration session and zero-volume session due to any reason. By default this command is disabled and system will not suppress any CDR.

Example

The following command configures the system to suppression the eG-CDR/P-CDRs created for a zero duration session or zero volume session:

```
gtpp suppress-cdrs zero-volume-and-duration egcdrs gcdrs
```

gtpp timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the CGF.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

[default] gtpp timeout *time*

default

Resets the systems GTPP timeout value to 20 seconds.

time

Specifies the maximum amount of time (in seconds) the system waits for a response from the CGF before assuming the packet is lost.
time is an integer from 1 through 60. Default: 20

Usage

This command works in conjunction with the **gtpp max-retries** command to establish a limit on the number of times that communication with a CGF is attempted before a failure is logged.
This parameter specifies the time between retries.

Example

The following command configures a retry timeout of 30 seconds:

```
gtpp timeout 30
```

gtpp trigger

Disables GTPP trigger conditions that cause either partial CDR record closure or opening of a new CDR record container. GTPP Triggers are specified in 3GPP TS 32.251 v6.6.0. All GTPP trigger changes take affect immediately, except **volume-limit**.

Product

ECS, GGSN, P-GW, S-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp trigger { cell-update | direct-tunnel | egcdr max-losdv | inter-plmn-sgsn-change |
ms-timezone-change | plmn-id-change | qos-change | rat-change [ generate { cdr |
container } ] | routing-area-update | sgsn-change-limit | serving-node-change-limit  |
tariff-time-change | time-limit | volume-limit }

default gtpp trigger

no gtpp trigger { cell-update | direct-tunnel | egcdr max-losdv | inter-plmn-sgsn-change
| ms-timezone-change | plmn-id-change | qos-change | rat-change | routing-area-update |
sgsn-change-limit | serving-node-change-limit | tariff-time-change | time-limit | volume-
limit }
```

default

Sets the specified trigger condition back to the default setting. All trigger conditions are enabled by default.

no

Re-enables the specified trigger condition.

cell-update

Enables the cell update trigger for S-CDRs, if the dictionary specified in the **gtpp dictionary** configuration includes support for cell update. This trigger is available only for 2G. Currently, custom18 dictionary supports the cell update trigger.

direct-tunnel

Enables the direct tunnel trigger for CDRs.

egcdr max-losdv

Enables the trigger for an eG-CDR/P-CDR if the List of Service Data Volume (LoSDV) containers crosses the configured limit for LOSDV containers. Default: Disabled

inter-plmn-sgsn-change

This keyword is for GGSN only.
Disabling this trigger ignores an Inter-PLMN SGSN change and doesn't release a G-CDR. Default: Enabled

ms-timezone-change

This keyword is specific to GGSN.
No partial record closure for a time zone change occurs when this trigger is disabled. MS time zone change should be applicable only for 3GPP R6 based GTPP dictionaries. Default: Enabled

plmn-id-change

This trigger keyword is specific to the 2G SGSN and is proprietary (non-standard).
Enables the PLMNID change trigger for S-CDRs if the dictionary specified in the **gtpp dictionary** configuration supports the PLMNID change. If enabled, the SGSN generates a partial S-CDR when the MS changes the PLMN while under the same SGSN (intra-system intra-SGSN PLMN-ID handover). Currently, custom18 dictionary supports this trigger. Default: Disabled

qos-change

Enables the QoS-change trigger for CDRs. Disabling this trigger ignores a QoS-change and does not open a new CDR for it. Default: Enabled

rat-change [generate { cdr | container }]

Enables or disables the partial record closure for a RAT change. If disabled, no partial record closure for a RAT change occurs. RAT change should be applicable only for 3GPP R6 based GTPP dictionaries. Default: Enabled
In SGSN, RAT change trigger (2G<->3G) means inter-service handoff (SGSN service <-> GPRS service). If this trigger is enabled, after the RAT change interim CDR is generated. After this RAT change CDR, CDR thresholds such as volume/time etc. and GTPP Group are applicable from new service. If RAT change trigger is disabled, the CDR thresholds and GTPP group etc. will not change and will continue to use from old service.
After the RAT change, the System Type field in CDR changes to indicate the new system type. If this trigger is disabled, then the next CDR generated will indicate System Type, but the data count in the CDR does not necessarily belong to the system type indicated in CDR; instead, it may belong to both 2G and 3G as CDR is not closing when handover takes place.

Important: the System Type field in CDR-related change is not applicable to customized CDR formats, which does not use the System Type field

generate { cdr | container }: Sets generation of CDR or just a Container on a RAT change.
cdr: Generates a CDR on a RAT-change.
container: Generates a container only on a RAT-change.

routing-area-update

Enables the routing-area-update trigger for CDRs.

sgsn-change-limit [also-intra-sgsn-multiple-address-group-change]

This keyword is obsolete and is available to maintain the backward compatibility for existing customers. The new keyword for **sgsn-change-limit** is **serving-node-change-limit**. Default: Enabled
Disabling this trigger ignores an SGSN change and does not add the SGSN IP address into the SGSN address list of the CDR. This helps to reduce the release of CDRs due to SGSN changes crossing the configured limit.
also-intra-sgsn-multiple-address-group-change: This keyword includes Intra-SGSN group changes as an SGSN change.

serving-node-change-limit [also-intra-sgsn-multiple-address-group-change]

This keyword is enabled for PGW, SGW, and GGSN. However, the **also-intra-sgsn-multiple-address-group-change** is enabled only for GGSN. Default: Enabled
Disabling this trigger ignores an SGSN change and does not add the SGSN IP address into the SGSN address list of the CDR. This helps to reduce the release of CDRs due to SGSN changes crossing the configured limit.
also-intra-sgsn-multiple-address-group-change: This keyword includes Intra-SGSN group changes as an SGSN change.

tariff-time-change

When this trigger is disabled, container closure does not happen for a tariff-time change. Default: Enabled
This trigger is applicable for G-MB-CDRs for MBMS session too.

time-limit

When this trigger is disabled, no partial record closure occurs when the configured time limit is reached. Default: Enabled
This trigger is applicable for G-MB-CDRs for MBMS session too.

volume-limit

When this trigger is disabled no partial record closure occurs when volume limit is reached. Default: Enabled
This trigger is applicable for G-MB-CDRs for MBMS session too.

Usage

Use this command to disable or re-enable GTTP triggers that can cause partial CDR record closure or cause a new CDR to be created.

Example

The following command disables partial record closure when a configured time limit is reached:

```
gtpp trigger time-limit
```

The following command re-enables partial record closure when a configured time limit is reached:

```
no gtpp trigger time-limit
```

gtpp transport-layer

Selects the transport layer protocol for Ga interface for communication between AGW (GSNs) and GTPP servers.

Product

GGSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gtpp transport-layer { tcp | udp }

default gtpp transport-layer
```

default

Resets the transport layer protocol to GTPP servers to the default of UDP.

tcp

Enables the system to implement TCP as transport layer protocol for communication with GTPP server.
Default: Disabled

udp

Enables the system to implement UDP as transport layer protocol for communication with GTPP server.
Default: Enabled

Usage

Use this command to select the TCP or UDP as the transport layer protocol for Ga interface communication between GTPP servers and AGWs (GSNs).

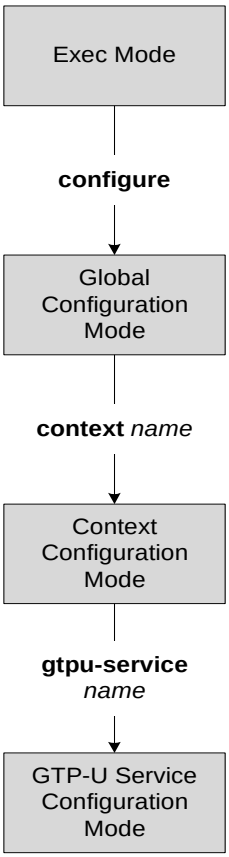
Example

The following command enables TCP as the transport layer protocol for the GSN's Ga interface.

```
gtpp transport-layer tcp
```

Chapter 138
GTP-U Service Configuration Mode Commands

The GTP-U Service Configuration Mode is used to manage parameters applied to incoming GTP-U packets.



bind

Configures the IP address to use for GTP-U data packets.

Product

GGSN, P-GW, S-GW

Privilege

Administrator

Syntax

[no] bind { ipv4-address *ipv4_address* **[crypto-template** *crypto_template* **] [ike-bind-address { ipv4_address }] [ipv6-address** *ipv6_address* **] | ipv6-address** *ipv6_address* **[crypto-template** *crypto_template* **] [ike-bind-address {** *ipv6_address* **}] [ipv4-address** *ipv4_address* **] }**

no

removes a configured IP address from this service.

ipv4-address *ipv4_address*

Binds this service to the IPv4 address of a configured interface.
ipv4_address must be entered using IPv4 dotted-decimal notation.

ipv6-address *ipv6_address*

Binds this service to the IPv6 address of a configured interface.
ipv6_address must be entered using IPv6 colon-separated notation.

crypto-template *crypto_template*

Configures crypto template for IPSec, which enables IPSec tunneling for this GTP-U address. Must be followed by the name of an existing crypto template.
crypto_template must be an alphanumeric string of 1 through 127 characters.

ike-bind-address *ip_address*

Configures an IKE bind address. Must be followed by IPv4 or IPv6 address; IP address type must be the same as the GTP-U address type.
ipv4_address must be entered using IPv4 dotted-decimal notation.
ipv6_address must be entered using IPv6 colon-separated notation.

Important: This keyword is only applicable if a crypto template is bound to the GTP-U address.

Usage

Use this command to bind the service to an interface for sending/receiving GTP-U packets.

Important: A GTP-U service can support a maximum of 12 GTP-U endpoints/interfaces.

Example

The following command configures the IPv4 address for this GTP-U service as *10.2.3.4*:

```
bind ipv4-address 10.2.3.4
```

echo-interval

Configures the rate at which GPRS Tunneling Protocol (GTP) v1-U echo packets are sent.

Product

GGSN, P-GW, S-GW

Privilege

Administrator

Syntax

echo-interval *seconds*

[default | no] echo-interval

seconds

Specifies the number of seconds between the sending of a GTP-Uv1 echo packet. *seconds* must be an integer from 60 through 3600.

default

Returns the command to its default setting of disabled.

no

Removes the configured echo-interval setting.

Usage

Use this command to configure the rate at which GTP-Uv1 echo packets are sent.

Example

The following command sets the rate between the sending of echo packets at *120* seconds:

```
echo-interval 120
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

extension-header

Configures the addition of an extension header in the GTP-U packet header, allowing for error indication messages.

Product

GGSN, P-GW, S-GW

Privilege

Administrator

Syntax

```
[ default | no ] extension-header source-udp-port
```

default

Returns the command to its default setting of disabled.

no

Disables the feature.

source-udp-port

Configures extension header type UDP Port support in GTP-U header for GTP-U Error Indication messages.

Usage

Use this command to configure the addition of an extension header in the GTP-U packet to allow for error indication messages

Example

The following command enables the inclusion of an extension header to allow for error indication messages:

```
extension-header source-udp-port
```

ipsec-allow-error-ind-in-clear

Configures whether error-indication is dropped or sent without IPSec tunnel.

Product

S-GW

Privilege

Administrator

Syntax

```
[ default | no ] ipsec-allow-error-ind-in-clear
```

default

Error-indication is dropped if no IPSec tunnel is present for that peer.

no

Disables the feature.

Usage

Use this command to determine whether error-indication is dropped or sent without an IPSec tunnel.
On receiving data packets for a session that does not exist, error-indication needs to be sent back to the peer. If there is no IPSec tunnel present with that peer, error-indication may be either dropped or sent without any IPSec tunnel.

Example

The following command allows error-indication to be sent without any IPSec tunnel:

```
ipsec-allow-error-ind-in-clear
```

ipsec-tunnel-idle-timeout

Configures the IPSec tunnel idle timeout after which IPSec tunnel deletion is triggered.

Product

S-GW

Privilege

Administrator

Syntax

ipsec-tunnel-idle-timeout *seconds*

default ipsec-tunnel-idle-timeout

seconds

Default: 60
Specifies the number of seconds an IPSec tunnel is idle before tunnel deletion is triggered. *seconds* must be an integer from 10 through 600.

default

Returns the command to its default setting of 60.

Usage

When there are no bearers on a particular IPSec tunnel, GTPUMGR initiates the delete for that tunnel. This timer helps to avoid unnecessary IPSec tunnel deletions for an idle tunnel.

Example

The following command sets the IPsec tunnel idle timeout to *100* seconds:

```
ipsec-tunnel-idle-timeout 100
```

max-retransmissions

Configures the maximum retry limit for GTP-U echo retransmissions.

Product

GGSN, P-GW, S-GW

Privilege

Administrator

Syntax

max-retransmissions *num*

no max-retransmissions

num

Default: 4
Specifies the number of GTP-U echo message retransmissions allowed before triggering a path failure error condition. *num* must be an integer from 0 through 15.

no

Disables the feature.

Usage

Use this command to set the maximum number of GTP-U echo message retransmissions in order to define a limit that triggers a path failure error.

Example

The following command sets the maximum GTP-U echo message retransmissions for this service to *10*:

```
max-retransmissions 10
```

path-failure detection-policy

Configures a path failure detection policy on GTP-U echo messages that have been retransmitted the maximum number of retry times.

Product

GGSN, P-GW, S-GW

Privilege

Administrator

Syntax

```
path-failure detection-policy gtp echo

[ default | no ] path-failure detection-policy
```

gtp echo

Sets the detection policy to detect a failure upon reaching the maximum number of GTP-U echo message retransmissions.

default

Resets the command to its default setting of enabled.

no

Disables the feature.

Usage

Use this command to set the detection policy for path failures.

Example

The following command sets the path failure detection policy to detect failures upon reaching the maximum number of GTP-U echo message retries:

```
path-failure detection-policy gtp echo
```

retransmission-timeout

Configures retransmission timeout for GTPU echo message retransmissions for this service.

Product

GGSN, P-GW, S-GW

Privilege

Administrator

Syntax

retransmission-timeout *seconds*

default retransmission-timeout

seconds

Default: 5
Specifies the number of seconds between the re-sending of GTP-U echo messages. *seconds* must be an integer from 1 through 20.

default

Returns the command to its default setting of 5.

Usage

Use this command to set the number of seconds between the retransmission of GTP-U echo messages.

Example

The following command sets the number of seconds between the sending of GTP-U echo messages to 7:

```
retransmission-timeout 7
```

sequence-number

Enables addition of the sequence number to every GTP-U packet. Default is disabled.

Product

GGSN, HSGW, P-GW, S-GW

Privilege

Administrator

Syntax

```
[ no ] sequence-number
```

no

Disables addition of the sequence number to every GTP-U packet.

Usage

Use this command to enable/disable addition of the sequence number to every GTP-U packet coming from Gi interface and going towards Gn/Gp interface. If GTP-U packets are received out of sequence, sequence numbers would allow the packets to be reorded.

Example

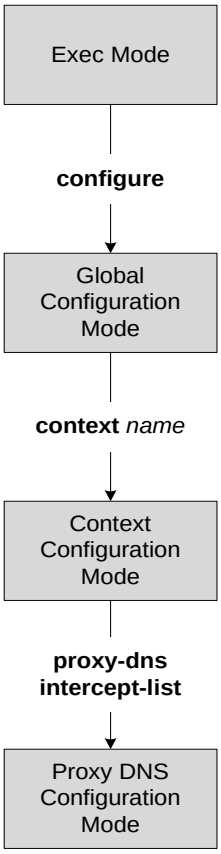
The following command enables addition of the sequence number to every GTP-U packet:

```
sequence-number
```

Chapter 139
HA Proxy DNS Configuration Mode Commands

The HA Proxy DNS Configuration Mode is used to create rules for Home Agent (HA) proxy DNS intercept lists that redirect packets with unknown foreign DNS addresses to a home network DNS server.

Important: HA Proxy DNS Intercept is a license-enabled feature.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

pass-thru

Sets IP addresses that should be allowed through the proxy DNS intercept feature.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

[no] pass-thru *ip_address* [*/ip_mask*]

no

Removes the DNS IP address from the pass-thru rule.

pass-thru *ip_address* **[/***ip_mask* **]**

Specifies an DNS IP address that is allowed through the intercept feature.
ip_address [/*ip_mask*]: Specifies the IP address and network mask bits. *ip_address* [/*ip_mask*] is specified using IPv4 dotted decimal or IPv6 colon-separated notation. The mask bits are a numeric value which is the number of bits in the subnet mask (CIDR notation).

Usage

Use this command to identify DNS IP addresses that should be allowed through the intercept feature. For a more detailed explanation of the proxy DNS intercept feature, see the **proxy-dns intercept-list** command in the *Context Configuration Mode Commands* chapter. A maximum of 16 intercept rules (either **redirect** or **pass-thru**) are allow for each intercept list.

Important: To allow packets through that do not match either the **pass-thru** or **redirect** rules, set a **pass-thru** rule address as: 0.0.0.0/0. If a packet does not match either the **pass-thru** or **redirect** rule, the packet is dropped.

Example

The following command allows a foreign network's DNS with an IP address of *10.2.55.12* to avoid being redirected:

```
pass-thru 10.2.55.12
```

redirect

Redirects DNS IP addresses from foreign networks matching an IP address in this command to a home network DNS.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] redirect any [ primary-dns ip_address [ secondary-dns ip_address ] ]
```

no

Removes the DNS IP address from the redirect rule.

primary-dns *ip_address*

Specifies the IP address of the primary home network DNS.
ip_address is specified using IPv4 dotted-decimal or IPv6 colon-separated notation.

secondary-dns *ip_address*

Specifies the IP address of the secondary home network DNS.
ip_address is specified using IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to identify DNS IP addresses from foreign networks that are to be redirected to the home DNS. For a more detailed explanation of the Proxy DNS feature, see the proxy-dns intercept-list command in the *Context Configuration Mode Commands* chapter. A maximum of 16 intercept rules (either **redirect** or **pass-thru**) are allow for each intercept list.
Since this command is configured in the source context, the destination context containing the path to the home network DNS is identified using the Context Configuration Mode command **ip dns-proxy source-address**.

Important: If a packet does not match the **pass-thru** or **redirect** rule, the packet is dropped. If **primary-dns** or **secondary-dns** is not configured, DNS messages are redirected to the primary-dns-server (or the secondary-dns-server) configured for the subscriber OR inside the context.

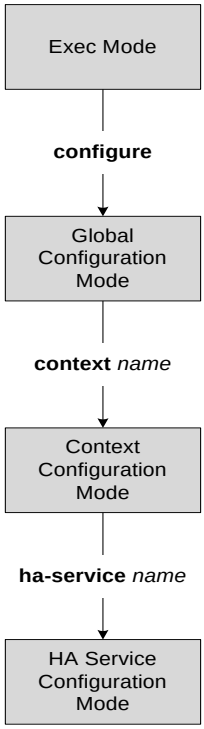
Example

The following command identifies a foreign network DNS with an IP address of *10.2.55.12* and redirects it to a primary home network DNS with an IP address of *10.3.4.5*:

```
predirect 10.2.55.12 primary-dns 10.3.4.5
```

Chapter 140
HA Service Configuration Mode Commands

The HA Service Configuration Mode is used to create and manage the Home Agent (HA) services within the current context.



a11-signalling-packets

Applies Differentiated Services Code Point (DSCP) marking for IP headers carrying outgoing signalling packets.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

a11-signalling-packets ip-header-dscp *ip-header-dscp***no a11-signalling-packets ip-header-dscpdefault a11-signalling-packets ip-header-dscp**

no

Disables DSCP marking for IP header encapsulation for the HA service.

default

Configures DSCP marking for IP header encapsulation for a specific HA service.

ip-header-dscp

Is a hexadecimal number between 0x0 and 0x3F.

Usage

The following command is used to apply DSCP marking for IP header carrying outgoing signalling packets.

Example

The following command applies DSCP marking for IP header carrying outgoing signalling packets.

```
a11-signalling-packets ip-header-dscp 0x2f
```

aaa

Configures the sending of subscriber session AAA accounting by the HA service.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
aaa { accounting [ roaming ] | group string }

no aaa { accounting | group }

default aaa accounting
```

no

Disables AAA accounting for the HA service.

default

Configures AAA parameters for specific HA service

accounting

accounting Enables the sending of AAA accounting information for subscriber sessions by the Home Agent (HA), by default is enabled.
roaming Enables the sending of AAA accounting information for subscriber sessions by the Home Agent (HA) only for roaming subscribers.

group

group configures aaa group for ha-service, **group** has lower priority than subscriber/apn config.
string: size ranges between *1* and *63*.

Usage

Enabling the HA service will send all accounting data (start, stop, and interim) to the configured AAA servers.
The chassis is shipped from the factory with the AAA accounting enabled.

Important: In order for this command to function properly, AAA accounting must be enabled for the context in which the HA service is configured using the aaa accounting subscriber radius command.

Example

The following command disables aaa accounting for the HA service:
no aaa accounting

access-network

Configures a specific access network configuration.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

access-network accounting identifier *access_network_accounting_identifier***no access-network accounting identifier**

no

Disables a specific access network configuration.

---

accounting

Specifies an access network configuration for accounting

identifier

Specifies an access network accounting identifier

access_network_accounting_identifier

This is an alphanumeric string of 1 through 128 characters.

Usage

This command is used to configure an access network for accounting.

Example

The following command configures an access network for accounting with the identifier *idnt*:
access-network accounting identifier idnt

associate

Associates an HA-service with a QoS policy.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

associate qci-qos-mapping *string***no associate qci-qos-mapping**

no

Disables the association of an HA-service with a QoS policy.

qci-qos-mapping *string*

Maps a QoS Class Identifier (QCI) for this HA service.

string is an alphanumeric string of 1 through 63 characters.

Usage

This command associates an HA-service with a QoS policy.

Example

The following command associates an HA-service with a QCI *map01*.

associate qci-qos-mapping map01

authentication

Configures authentication parameters for a specific HA service within a context.

Product

HA, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

```
authentication {aaa-distributed-mip-keys [ disabled | optional | required ]|dmu-refresh-
key | imsi-auth| mn-aaa {allow-noauth  | always| dereg-noauth | noauth | renew-reg-noauth
| renew-and-dereg-noauth } | mn-ha { allow-noauth | always } | pmip-auth | stale-key-
disconnect }

no authentication {imsi-auth | pmip-auth }

default authentication { aaa-distributed-mip-keys |  dmu-refresh-key |  imsi-auth |  mn-
aaa |  mn-ha |  pmip-auth | stale-key-disconnect }
```

no

Disable the parameter.

default

Resets the specified option to its default setting.

aaa-distributed-mip-keys [disabled | optional |required]

Configures use of AAA distributed MIP keys for authenticating RRQ for WiMAX HA calls.
Default is disabled.
disabled: Disables using AAA distributed WiMAX Mobile IP (MIP) keys for authenticating MIP RRQ.
optional: Uses AAA distributed WiMAX MIP keys for authenticating RRQ with fallback option to use static/3GPP2 based MIP keys.
required: AAA distributed WiMAX MIP keys for authenticating MIP RRQ are mandatory

dmu-refresh-key

Typically, when a Dynamic Mobile IP Update (DMU) resets, the next MIP re-registration causes MN-HA authorization failure and the HA rejects the MIP RRQ. This parameter enables the HA to retrieve the MN-HA key again from the AAA during the call and to use the freshly retrieved key value to recheck authentication.
Default is disabled.

imsi-auth

Enable uses the International Subscriber Mobile identity (IMSI) to determine if MN-AAA or MN-FAC extensions are not present in the RRQ.
Default is disabled.

mn-aaa { allow-noauth | always | dereg-noauth | noauth | renew-reg-noauth | renew-and-dereg-noauth }

Specifies how mobile node-to-AAA authentication extension in registration requests from the mobile node should be handled by the HA service.
Default is always.
allow-noauth: Specifies that the HA service does not require authentication for every mobile node registration request. However, if the mn-aaa extension is received, the HA service will authenticate it.
always: Specifies that the HA service will perform authentication each time a mobile node registers.
dereg-noauth: Disables authentication request upon de-registration.
noauth: Specifies that the HA service will not look for mn-aaa extension and will not authenticate it.
renew-reg-noauth: Specifies that the HA service will not perform authentication for mobile node re-registrations. Initial registration and de-registration will be handled normally.
renew-and-dereg-noauth: Disables authentication request upon re-registration and de-registration.

mn-ha { allow-noauth | always }

Specifies whether the HA service looks for an MN-HA authentication extension in the RRQ.
Default is always.
allow-noauth: Allows a request that does not contain the auth extension.
always: A request should always contain the auth extension to be accepted.

pmip-auth

Specifies whether the HA service looks for an MN-HA authentication extension in the RRQ.
Default is always.
allow-noauth: Allows a request that does not contain the auth extension.
always: A request should always contain the auth extension to be accepted.

stale-key-disconnect

If MN-HA auth fails for MIP renew and dereg, disconnects the call immediately.
Disabled by default.

Usage

The **authentication** command, combined with a keyword, can be used to specify how the system will perform authentication of registration request messages.

Example

The following command configures the HA service to always perform mobile node authentication for every registration request.

```
authentication mn-aaa always
```

The following command configures the HA service to always look for an MN-HA authentication extension in the RRQ.

```
authentication mn-ha always
```

bind

Binds the HA service to a logical IP interface serving as the Pi interface and specifies the maximum number of subscribers that can access this service over the interface.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
bind address address [ max-subscribers count ]
no bind address
```

address

Specifies the IP address (address) of the interface configured as the Pi interface. *address* is specified in IPv4 dotted-decimal notation.

max-subscribers *count*

Default: *500000*
Specifies the maximum number of subscribers that can access this service on this interface.
count can be configured to an integer from 0 through 4000000.

Important: The maximum number of subscribers supported is dependant on the license key installed and the number of active packet processing cards installed in the system.

Usage

Associate the HA service to a specific logical IP address. The logical IP address or interface takes on the characteristics of a Pi interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.
This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.
When configuring the **max-subscribers** option, be sure to consider the following:

- The total number of interfaces that you will configuring for use as Pi interfaces
- The maximum number of subscriber sessions that all of these interfaces may handle during peak busy hours
- The average bandwidth for each of the sessions
- The type of physical port to which these interfaces will be bound

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.
Use the **no bind address** command to delete a previously configured binding.

Example

The following command would bind the logical IP interface with the address of *192.168.3.1* to the HA service and specifies that a maximum of *600* simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```
bind address 192.168.3.1 max-subscribers 600
```

The following command disables a binding that was previously configured:

```
no bind address
```

encapsulation

Configures Mobile IP (MIP) encapsulation types supported for a specific HA service.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] encapsulation allow { gre | keyless-gre }
```

no

Disables MIP encapsulation types supported for specific HA service

allow

Allows encapsulation type for MIP data.

gre

Default: Enabled.
Specifies the use of Generic Routing Encapsulation (GRE) for MIP data.

keyless-gre

Default: Disabled.
Specifies the use of GRE without exchanging keys for MIP data.

Usage

Use to disable or re-enable the use of GRE encapsulation or Key-less encapsulation for MIP sessions.
In case of chassis HA operating with other vendor equipment, which does not support the 3GPP2 to exchange key, this command with **keyless-gre** keyword will make the chassis HA to accept MIP data with legacy GRE.

Example

To disable GRE for MIP sessions, enter the following command:

```
no encapsulation allow gre
```

To re-enable GRE for MIP sessions, enter the following command:

```
encapsulation allow gre
```

To enable key-less GRE for MIP sessions, enter the following command:

```
encapsulation allow keyless-gre
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

fa-ha-spi

Configures the security parameter index (SPI) for specific HA service parameters.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

fa-ha-spi remote-address { *fa_ip_address* | *fa_ip_address_mask* } **spi-number** *number* { **encrypted secret** *enc_secret* | **secret** *secret* } [**allow-fa-ha-auth-extension**] [**description** *string*] [**disallow-fa-ha-auth-extension**] [**hash-algorithm** { **hmac-md5** | **md5** | **rfc2002-md5** }] [**replay-protection** { **nonce** | **timestamp** [**timestamp-tolerance tolerance**] }] [**timestamp-tolerance** *tolerance*]

no fa-ha-spiremote-address { *ha_ip_address* | *ha_ip_address/mask* }**spi-number** *number*

no

Disables the security parameter index (SPI) for specific HA service parameters.

remote-address { *fa_ip_address* | *fa_ip_address/mask* }

Specifies the IP address of the FA. *fa_ip_address* is entered using IPv4 dotted-decimal notation with CIDR for the subnet mask.

Important: The system supports unlimited peer FA addresses per HA but only maintains statistics for a maximum of 8,192 peer FAs. If more than 8,192 FAs are attached, older statistics are overwritten.

spi-number *number*

Specifies the SPI (number) which indicates a security context between the FA and the HA in accordance with RFC 2002.
number is an integer value from 256 through 4294967295.

encrypted secret *enc_secret* **| secret** *secret*

Configures the shared-secret between the HA service and the FA. The secret can be either encrypted or non-encrypted.
encrypted secret *enc_secret*: Specifies the encrypted shared key between the HA service and the FA. *enc_secret* must be an alphanumeric string of 1 through 236 characters that is case sensitive.
secret *secret*: Specifies the shared key between the HA service and the FA. *secret* must be an alphanumeric string of 1 through 236 characters that is case sensitive.

allow-fa-ha-auth-extension

Allows validation of FA HA Authentication extension.

description *string*

This is a description for the SPI. *string* must be an alphanumeric string of 0 through 31 characters.

hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }

Default: hmac-md5
Specifies the hash-algorithm used between the HA service and the FA.
hmac-md5: Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis.
md5: Configures the hash-algorithm to implement MD5 per RFC 1321.
rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

replay-protection { timestamp [timestamp-tolerance *tolerance* **]| nonce }**

Specifies the replay-protection scheme that should be implemented by the FA service for this SPI.
nonce: Configures replay protection to be implemented using NONCE per RFC 2002.
timestamp: Configures replay protection to be implemented using timestamps per RFC 2002.
timestamp-tolerance: Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. *tolerance* is measured in seconds and can be configured to an integer from 1 and 65535. The default is 60.

Usage

An SPI is a security mechanism configured and shared by the HA service and the FA. Please refer to RFC 2002 for additional information.
Though it is possible for FAs and HAs to communicate without SPIs being configured, the use of them is recommended for security purposes. It is also recommended that a "default" SPI with a remote address of 0.0.0.0/0 be configured on both the HA and FA to prevent hackers from spoofing addresses.

Important: The SPI configuration on the HA must match the SPI configuration for the FA service on the system in order for the two devices to communicate properly.

A maximum of 2,048 SPIs can be configured per HA service.
Use the **no** version of this command to delete a previously configured SPI.

Example

The following command configures the FA service to use an SPI of *512* when communicating with an HA with the IP address *192.168.0.2*. The key that would be shared between the HA and the FA service is *q397F65*. When communicating with this HA, the FA service will also be configured to use the rfc2002-md5 hash-algorithm.

```
fa-ha-spi remote-address 192.168.0.2 spi-number 512 secret q397F65 hash-
algorithm rfc2002-md5
```

The following command deletes the configured SPI of 400 for an HA with an IP address of *172.100.3.200*:

```
no fa-ha-spi remote-address 172.100.3.200 spi-number 400
```

gre

Configures Generic Routing Encapsulation (GRE) parameters.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

gre { **checksum** | **checksum-verify** | **reorder-timeout** *timeout* | **sequence-mode** { **none** | **reorder** } | **sequence-numbers** }

default gre { **checksum** | **checksum-verify** | **reorder-timeout** | **sequence-mode** | **sequence-numbers** }**no gre** { **checksum** | **checksum-verify** | **sequence-numbers** }

no

Disables the specified functionality.

default

Sets or restores default value assigned for specified parameter.

checksum

Default: disabled
Enables the introduction of the checksum field in outgoing GRE packets.

checksum-verify

Default: disabled
Enables verification of the GRE checksum (if present) in incoming GRE packets.

reorder-timeout *timeout*

Default: 100
Configures the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets. *timeout* must be an integer from 0 through 5000.

sequence-mode { none | reorder }

Default: none
Configures how incoming out-of-sequence GRE packets should be handled.
none: Disables reordering of incoming out-of-sequence GRE packets.
reorder: Enables reordering of incoming out-of-sequence GRE packets.

sequence-numbers

Default: Disabled
Enables the insertion of sequence numbers into the GRE packets.

Usage

Use this command to configure how the HA service handles GRE packets.

Example

To set the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets to *500* milliseconds, enter the following command:

```
gre reorder-timeout 500
```

To enable the reordering of incoming out of sequence GRE packets, enter the following command:

```
gre sequence-mode reorder
```

To enable the insertion or removal of GRE sequence numbers in GRE packets, enter the following command:

```
gre sequence-numbers
```

idle-timeout-mode

Configures the sessions idle-timer reset behavior.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
idle-timeout-mode { aggressive | handoff | normal } [ upstream-only ]

default idle-timeout-mode
```

default

Resets the idle timeout mode to the default settings.

aggressive

Resets the session idle timer only when MIP user data is detected. This is the default behavior.

handoff

Resets the session idle timer when MIP user data is detected and an inter-Access Gateway/FA handoff occurs.

normal

Resets the session idle timer when MIP user data is detected and any MIP control signaling occurs.

upstream-only

Only upstream user data (data from the mobile node) resets the idle timer for the session. This is disabled by default.

Usage

Use this command to set how the current HA service resets the idle timer for a session.

Example

To reset the idle timer whenever user data is detected or whenever an inter-Access Gateway/FA occurs, use the following command:

```
idle-timeout-mode handoff
```

ikev1

Configures IPSec Internet Key Exchange (IKE) parameters.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

ikev1 { **aaa-context** *aaa_context_string* | **peer-fa** *IPAddress* **crypto-map** *crypto_map_string* [**encrypted**] [**secret** *secret_string*] | **skew-lifetime** *seconds* } **no ikev1** { **aaa-context** | **peer-fa** *IPAddress* | **skew-lifetime** }

no

Disables IPSec IKE parameters.

aaa-context *aaa_context_string*

Configures AAA context from which to retrieve IKE keys. Must be followed by the context name.

aaa_context_string is an alphanumeric string of 1 through 63 characters.

peer-fa *IPAddress*

Sets the IKE crypto-map for a peer Foreign Agent (FA).

IPAddress is IP address entered using IPv4 dotted-decimal or IPv6 colon-separated notation.

crypto-map *crypto_map_string*

Configures IKE crypto-map. Must be followed by the crypto-map name.

crypto_map_string is an alphanumeric string of 1 through 63 characters.

encrypted designates use of encryption

secret *secret_string* uses a secret that is shared between FA and HA. *secret_string* is an alphanumeric string of 1 through 256 characters.

skew-lifetime *seconds*

Configures the "S" lifetime Skew (in seconds). *seconds* is an integer from 1 through 65534. Default is 10.

Usage

Use this command to configure IPSec IKE parameters.

Example

ikev1 peer-fa 11.22.33.44 crypto-map er encrypted secret ert

ip context-name

Specifies name of the destination context to be applied to the subscribers.

This configuration overrides the local subscriber configuration as well as the return attributes sent by RADIUS. All calls coming to this HA service are assigned this destination context; the IP address is allocated from the specified IP pool or group that is configured in the context specified in the service.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

ip context-name *name*

no ip context-name

default ip context-name

name

Specifies the name of the context to assign the subscriber to once authenticated. *name* must be an alphanumeric string from 1 through 79 characters.

no

Usage

Removes the current assigned context from the subscriber's data.Set the name of the destination context to be applied to the subscribers.

Example

```
ip context-name sampleName
no ip context-name
```

ip local-port

Configures the local User Datagram Protocol (UDP) port for the Pi interface's IP socket on which to listen for Mobile IP Registration messages.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

ip local-port *number*

default ip local-port

default

Sets or restores the default value assigned for the IP local port.

number

Specifies the UDP port number.
number is an integer from 1 through 65535. Default is 434.

Usage

Specify the UDP port that should be used for communications between the FA service and the HA.

Example

The following command specifies a UDP port of *3950* for the HA service to use to communicate with the HA on the Pi interface:

```
ip local-port 3950
```

ip pool

Specifies name of the IP address pool or group to use for subscriber IP address allocation.

This configuration overrides the local subscriber configuration, as well as the return attributes sent by RADIUS. All calls coming to this HA service are assigned this destination context and an IP address is allocated from the specified IP pool or group that is configured in the context specified in the service.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

ip pool *name*

no ip pool

default ip pool

name

Specifies the logical name of the IP address pool. *name* must be an alphanumeric string of 1 through 31 characters.

no

Removes the specified IP address pool specified from the current context or disables the option for an IP pool.

default

Clears the IP address pool or group setting.

Usage

Define a pool of IP addresses for the context to use in assigning IPs for this service.

Example

The specifies name of the IP address pool or group to use for subscriber IP address allocation:

```
ip pool pool1
```

The following command removes the specified IP address pool:

```
no ip pool pool1
```

min-reg-lifetime

Configures Mobile IP session minimum registration lifetime, in seconds.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

[no | default] min-reg-lifetime *min_reg_lifetime_seconds*

no

Disables the min registered lifetime.

default

Configures Mobile IP session minimum registration lifetime to default which is *0*.

min-reg-lifetime

Configures Mobile IP session minimum registration lifetime.

min_reg_lifetime_seconds

Variable in the range between *1* and *65534*.

Usage

Use this command to configure Mobile IP session minimum registration lifetime, in seconds, between *1* and *65534*. Default is *0* seconds.

Example

Use the following command to configure mobile IP session to minimum registered life time to *100* seconds:

min-reg-lifetime *100*

mn-ha-spi

Configures the security parameter index (SPI) between the HA service and the mobile node (MN).

Product

HA

Privilege

Security Administrator, Administrator

Syntax

mn-ha-spi spi-number *number* [**description** *string*] [**encrypted secret** *enc_secret*] [**hash-algorithm** { **hmac-md5** | **md5** | **rfc2002-md5** }] [**permit-any-hash-algorithm**] [**replay-protection** { **nonce** | **timestamp** }] [**secret** *secret*] [**timestamp-tolerance** *tolerance*]

no mn-ha-spi spi-number *number*

spi-number *number*

Specifies the SPI (number) which indicates a security context between the mobile node and the HA service in accordance with RFC 2002. *number* can be configured to an integer from 256 through 4294967295.

description *string*

This is a description for the SPI. *string* is an alphanumeric string of 1 through 31 characters.

encrypted secret *enc_secret* **| secret** *secret*

Configures the shared-secret between the HA service and the mobile node. The secret can be either encrypted or non-encrypted.
encrypted secret *enc_secret*: Specifies the encrypted shared key between the HA service and the mobile node. *enc_secret* must be an alphanumeric string of 1 through 254 characters that is case sensitive.
secret *secret*: Specifies the shared key between the HA service and the mobile node. *secret* must be an alphanumeric string of 1 through 127 characters that is case sensitive.
The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }

Default: hmac-md5
Specifies the hash-algorithm used between the HA service and the mobile node.
hmac-md5: Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis.
md5: Configures the hash-algorithm to implement MD5 per RFC 1321.
rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

permit-any-hash-algorithm

Default: disabled
Allows verification of the MN-HA authenticator using all other hash-algorithms after failure with configured hash-algorithm. The successful algorithm is logged to aid in troubleshooting and used to create the MN-HA authenticator in the Registration Reply message.

replay-protection { nonce | timestamp }

Default: timestamp
Specifies the replay-protection scheme that should be implemented by the HA service for this SPI.
nonce: configures replay protection to be implemented using NONCE per RFC 2002.
timestamp: configures replay protection to be implemented using timestamps per RFC 2002.

timestamp-tolerance *tolerance*

Default: *60*
Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. If this is set to *0*, timestamp tolerance checking is disabled at the receiving end.
Tolerance is measured in seconds and can be configured to an integer from 0 through 65535.

Usage

An SPI is a security mechanism configured and shared by the HA service and the mobile node. Please refer to RFC 2002 for additional information.
Use the **no** version of this command to delete a previously configured SPI.

Example

The following command configures the HA service to use an SPI of 640 when communicating with a mobile node. The key that would be shared between the mobile node and the HA service is q397F65.

```
mn-ha-spi spi-number 640 secret q397F65
```

The following command deletes the configured SPI of *400*:

```
no mn-ha-spi spi-number 400
```

nat-traversal

This command enables NAT traversal and also configures the forcing of UDP tunnels for NAT traversal.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
nat-traversal [force-accept]

no nat-traversal [force-accept]

default nat-traversal [force-accept]
```

no

Disables NAT traversal or disables forcing the acceptance of UDP tunnels for NAT traversal.

default

Reset the defaults for this command.
Default: NAT traversal disabled, force-accept disabled.

force-accept

This keyword configures the HA to accept requests when NAT is not detected but the Force (F) bit is set in the RRQ with the UDP Tunnel Request. By default this type of request is rejected if NAT is not detected.

Usage

Use this command to enable NAT traversal and enable the forcing of UDP tunnels for NAT traversal.

Example

The following command enables NAT traversal for the current HA service and forces the HA to accept UDP tunnels for NAT traversal:

```
nat-traversal force-accept
```

optimize tunnel-reassembly

Designates that tunnel reassembly optimization will be used for fragmented large packets passed between HA and FA. Default is disabled.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
optimizetunnel-reassembly

no optimize tunnel-reassembly

default optimize tunnel-reassembly
```

Usage

Enabling this functionality fragments large packets prior to encapsulation for easier processing. Tunnel reassembly optimization is disabled by default.

Important: You should not use this command without first consulting Cisco Systems Technical Support. This command applies to very specific scenarios where packet reassembly is not supported at the far end of the tunnel. There are cases where the destination network may either discard the data, or be unable to reassemble the packets.

Important: This functionality works best when the HA service is communicating with an FA service running in a system. However, an HA service running in the system communicating with an FA from a different manufacturer will operate correctly even if this parameter is enabled.

Use the **no** version of this command to disable tunnel optimization if enabled.

Example

The following command enables tunnel reassembly optimization:

```
optimize tunnel-reassembly
```

per-domain statistics-collection

Enables per-domain statistics collection.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
per-domain statistics-collectionno per-domain statistics-collection
```

Usage

Use this command to enable per-domain statistics collection.

Example

The following command enables per-domain statistics collection.

```
per-domain statistics-collection
```

policy bc-query-result

Configure the binding cache (BC) query Response Result code.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

policy bc-query-result network-failure *code*

default policy bc-query-resultnetwork-failure

network-failure *code*

Default: *0xFFFF*
Specify the response code for BC responses sent on network failures.
code must be either 0xFFFF or 0xFFFE.

Usage

Use this command to specify the type of response code to send in a P-MIP BC query result.

Example

The following command sets the P-MIP BC query result response code to *0xFFFE*:

```
policy bc-query-result network-failure 0xFFFE
```

policy nw-reachability-fail

Specifies the action to take upon detection of an up-stream network -reachability failure.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

policy nw-reachability-fail { **redirect** *ip_addr1* [**weight** *value*] [ip_addr2 [**weight** *value*] ... *ip_addr16* [**weight** *value*]] | **reject** [**use-reject-code** { **admin-prohibited** | **insufficient-resources** }] }

no policy nw-reachability-fail [**redirect** *ip_addr1 ... ip_addr16*]

no

Deletes the network reachability policy completely or deletes the specified redirect addresses fro the policy.

reject [use-reject-code { admin-prohibited | insufficient-resources }]

Upon network reachability failure, reject all new calls for this context.
use-reject-code { **admin-prohibited** | **insufficient-resources** }: When rejecting calls send the specified reject code. If this keyword is not specified the admin-prohibited reject code is sent by default.

reject [use-reject-code { admin-prohibited | insufficient-resources }]

Upon network reachability failure reject all new calls for this context. If no reject code is specified, the HA sends a registration reply code of 81H (admin-prohibited).
use-reject-code { **admin-prohibited** | **insufficient-resources** }: Use the specified reject code when rejecting traffic.
admin-prohibited: When this keyword is specified and traffic is rejected, the error code 81H (admin-prohibited) is returned.
insufficient-resources: When this keyword is specified and traffic is rejected, the error code 82H (insufficient resources) is returned.

redirect *ip_addr1* **[weight** *value* **] [ip_addr2 [weight** *value* **] ...** *ip_addr16* **[weight** *value* **]]**

Upon network reachability failure redirect all calls to the specified IP address.
ip_addr1: This must entered using IPv4 dotted-decimal notation. Up to 16 IP addresses and optional weight values can be entered on one command line.
weight *value*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. If a weight is not specified the entry is automatically assigned a weight of 1. *value* must be an integer from 1 through 10.

Usage

Use this command to set the action for the HA service to take upon a network reachability failure.

Important: Refer to the Context Configuration mode command **nw-reachability server** to configure network reachability servers.

Important: Refer to the Subscriber Configuration mode command **nw-reachability-server** to bind the network reachability to a specific subscriber.

Important: Refer to the **nw-reachability server server_name** keyword of the Context Configuration mode **ip pool** command to bind the network reachability server to an IP pool.

Example

To set the HA service to reject all new calls on a network reachability failure, enter the following command:

```
policy nw-reachability-fail reject
```

Use the following command to set the HA service to redirect all calls to the HA at IP address *192.168.100.10* and *192.168.200.10* on a network reachability failure:

```
policy nw-reachability-fail redirect 192.168.100.10 192.168.200.10
```

policy overload

Configures the overload policy within the HA service.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

policyoverload { **redirect***address* [**weight***weight_num*] [*address2* [**weight***weight_num*] ... *address16*[**weight***weight_num*]] | **reject**[**use-reject-code** { **admin-prohibited** | **insufficient-resources** }] }

no policyoverload [**redirect***address* [*address2...address16*]

---

no policy overload [redirect *address* **[** *address2...address16* **]]**

Deletes a previously set policy or removes a redirect IP address.
overload: Without any options deletes the complete overload policy from the PDSN service.
overload redirect *address* [*address2 ... address16*]: deletes up to 16 IP addresses from the overload redirect policy. The IP addresses must be expressed in IP v4 dotted-decimal notation

---

redirect *address* **[weight** *weight_num* **] [** *address2* **[weight** *weight_num* **] ...** *address16* **[weight** *weight_num* **]**

This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the HA service rejects new sessions with a Registration Reply Code of 136H (unknown home agent address) and provides the IP address of an alternate HA. This command can be issued multiple times.
address: The IP address of an alternate HA expressed in IP v4 dotted-decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy, the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.
weight *weight_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. *weight_num* must be an integer from 1 through 10.

---

reject [use-reject-code { admin-prohibited | insufficient-resources }]

This option causes any overload traffic to be rejected. If no reject code is specified, the HA sends a registration reply code of 81H (admin-prohibited).
use-reject-code { **admin-prohibited** | **insufficient-resources** }: Use the specified reject code when rejecting traffic.
admin-prohibited: When this keyword is specified and traffic is rejected, the error code 81H (admin-prohibited) is returned.
insufficient-resources: When this keyword is specified and traffic is rejected, the error code 82H (insufficient resources) is returned.

Usage

The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system.
The system automatically invokes the overload policy when an on-line software upgrade is started.
Use the **no** version of this command to restore the default policy.
The setting for overload policy is reject.

Example

The following command enables an overload redirect policy for the HA service that will send overload calls to either of two destinations with weights of *1* and *10* respectively:

```
policy overload redirect 192.168.100.10 weight 1 192.168.100.20 weight 10
```

reg-lifetime

Configures Mobile IP session registration lifetime.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

reg-lifetime *time*

no reg-lifetime

default reg-lifetime

no

Sets the registration lifetime to infinite.

default

Sets the registration lifetime to default value, 600.

time

Specifies the registration lifetime in seconds.
time is an integer from 1 through 65534.

Usage

Use this command o limit a mobile node's lifetime. If the mobile node requests a shorter lifetime than what is specified, it is granted. However, Per RFC 2002, should a mobile node request a lifetime that is longer than the maximum allowed by this parameter, the HA service will respond with the value configured by this command as part of the Registration Reply. The default is 600 seconds.

Example

The following command configures the registration lifetime for the HA service to be *2400* seconds:

```
reg-lifetime 2400
```

The following command configures an infinite registration lifetime for MIP calls:

```
no reg-lifetime
```

reverse-tunnel

Enables use of reverse tunneling for Mobile IP session. Use no reverse-tunnel command to disable. If disabled, mobile node (MN) packets are not tunneled to the HA in the reverse direction.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
reverse-tunnel

no reverse-tunnel

default reverse-tunnel
```

no

Indicates the reverse tunnel option is to be disabled. When omitted, the reverse tunnel option is enabled.

default

Indicates the reverse tunnel option is to be set to the default. When omitted, the reverse tunnel option is enabled.

Usage

Reverse tunneling involves tunneling datagrams originated by the mobile node to the HA service via the FA. When an MN arrives at a foreign network, it listens for agent advertisements and selects an FA that supports reverse tunnels. The MN requests this service when it registers through the selected FA. At this time, the MN may also specify a delivery technique such as Direct or the Encapsulating Delivery Style.
Among the advantages of using reverse-tunneling are that:

- All datagrams from the mobile node seem to originate from its home network
- The FA can keep track of the HA to which the mobile node is registered and tunnel all datagrams from the mobile node to its HA

Use the **no** version of this command to disable reverse tunneling. If reverse tunneling is disabled, and the mobile node does not request it, triangular routing will be performed.
Routing will be used.
The default setting is reverse tunnel enabled.

Important: If reverse tunneling is disabled on the system and a mobile node requests it, the call will be rejected with a reply code of 74H (reverse-tunneling unavailable).

Example

The following command disables reverse-tunneling support for the HA service:

```
no reverse-tunnel
```

revocation

Configures the Registration Revocation feature for a specific HA service.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
revocation { enable | max-retransmission number | negotiate-i-bit | retransmission-
timeout secs | send-nai-ext | trigger { handoff | idle-timeout } }

no revocation { enable | negotiate-i-bit | send-nai-ext | trigger { handoff | idle-
timeout } }

default revocation [ enable ] [ max-retransmission ] [ negotiate-i-bit ] [
retransmission-timeout ] [ send-nai-ext ] [ trigger { handoff | idle-timeout } ]
```

no

Completely disables registration revocation on the HA, disables trigger handoff, or disables revocation on idle timer expiration.

default

Sets or restores the default value assigned for specified parameter.

enable

Enables the MIP registration revocation feature on the HA. When enabled, if revocation is negotiated with an FA and a MIP binding is terminated, the HA can send a Revocation message to the FA. This feature is disabled by default.

max-retransmission *number*

Default: 3
The maximum number of retransmissions of a Revocation message before the revocation fails. *number* must be an integer from 0 through 10.

negotiate-i-bit

Default: disabled
Enables the HA to negotiate the i-bit via PRQ/RRP messages and processes the i-bit revocation messages.

retransmission-timeout *secs*

Default: 3
The number of seconds to wait for a Revocation Acknowledgement from the FA before retransmitting the Revocation message. *secs* must be an integer from 1 through 10.

send-nai-ext

Default: off

Enables sending the NAI extension in the revocation message.

trigger { handoff | idle-timeout }

handoff: Default: Enabled
Triggers the HA to send a Revocation message to the FA when an inter-Access Gateway/FA handoff of the MIP session occurs. If this is disabled, the HA is never triggered to send a Revocation message.
idle-timeout: Default: Enabled
Triggers the HA to send a Revocation message to the FA when a session idle timer expires.

Usage

Use this command to enable or disable the MIP revocation feature on the HA or to change settings for this feature. Both the HA and the FA must have Registration Revocation enabled and FA/HA authorization must be in use for Registration Revocation to be negotiated successfully.

Example

The following command enables Registration Revocation on the HA:

```
revocation enable
```

The following command sets the maximum number of retries for a Revocation message to *10*:

```
revocation max-retransmission 10
```

The following command sets the timeout between retransmissions to *3*:

```
revocation retransmission-timeout 3
```

The behavior of send MIP revocation to FA is as follows:

- 1st retry: Retransmit in 3 seconds after previous MIP revocation send.
- 2nd retry: Retransmit in 6 seconds after previous MIP revocation send (9 seconds after sending initial MIP revocation).
- 3rd retry: Retransmit in 12 seconds after previous MIP revocation send (21 seconds after sending initial MIP revocation).
- 4th retry: Retransmit in 24 seconds after previous MIP revocation send (45 seconds after sending initial MIP revocation).
- 5th retry: Retransmit in 48 seconds after previous MIP revocation send (93 seconds after sending initial MIP revocation).

Important: The value of retransmission-timeout doubles. HA disconnects the session forcibly in 120 seconds after sending initial MIP revocation.

setup-timeout

The maximum time allowed for session setup in seconds. Default is 60 seconds.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

setup-timeout *seconds*

default setup-timeout

default

Sets or restores the default value.

seconds

Default: 60 seconds
The maximum amount of time (in seconds) to allow for setup of a session. *seconds* must be an integer from 1 through 1000000

Usage

Use this command to set the maximum amount of time allowed for setting up a session.

Example

To set the maximum time allowed for setting up a session to 5 minutes (*300* seconds), enter the following command:

```
setup-timeout 300
```

simul-bindings

Specifies the maximum number of “care-of” addresses that can simultaneously be bound for the same user as identified by NAI and Home address.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

simul-bindings *number*

default simul-bindings

default

Sets or restores the default value.

number

Configures the maximum number of simultaneous “care-of” bindings that the HA service will maintain for any given subscriber.
is an integer from 1 through 3.

Usage

Per RFC 2002, the HA service creates a mobile binding record (MBR) for each subscriber session it is facilitating. Each MBR is associated with a care-of address. As the mobile node roams, it is possible that the session will be associated with a new care of address.
Typically, the HA service will delete an old binding and create a new one when the information in the Registration Request changes. However, the mobile could request that the HA maintain previously stored MBRs. This command allows you to configure the maximum number of MBRs that can be stored per subscriber if the requested. The default value is 3.

Example

The following command configures the HA service to support up to 4 MBRs per subscriber:

```
simul-bindings 4
```

threshold dereg-reply-error

Sets an alarm or alert based on the number of de-registration reply errors per HA service.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

threshold dereg-reply-error *high_thresh* [**clear** *low_thresh*]

no threshold dereg-reply-error

no

Deletes the alert or alarm.

high_thresh

Default: 0
Specifies the high threshold number of de-registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to an integer from 0 through 100000.

clear *low_thresh*

Default: 0
The low threshold number of de-registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to an integer from 0 through 100000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of de-registration reply errors is equal to or greater than a specified number of calls per second.
Alerts or alarms are triggered for the number of de-registration reply errors on the following rules:

- **Enter condition:** Actual number of de-registration reply errors > High Threshold
- **Clear condition:** Actual number of de-registration reply errors < Low Threshold

Example

The following command configures a de-registration reply error threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold reg-reply-error 1000 clear 500
```

threshold init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for the context.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
threshold init-rrq-rcvd-rate high_thresh [ clear low_thresh]
no threshold init-rrq-rcvd-rate
```

no

Deletes the alert or alarm.

high_thresh

Default: 0
Specifies the high threshold average number of calls setup per second that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 100000.

clear *low_thresh*

Default:0
The low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. *low_thresh* is an integer from 0 through 100000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the average number of calls setup per second is equal to or greater than a specified number of calls per second.
Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter condition:** Actual number of calls setup per second is greater than the high threshold.
- **Clear condition:** Actual number of calls setup per second is less that the low threshold.

Example

The following command configures a number of calls setup per second threshold of 1000 and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold init-rrq-rcvd-rate 1000 clear 500
```

threshold ipsec-call-req-rej

Configures a threshold for the total IPSec calls request rejected.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

threshold ipsec-call-req-rej *high_thresh* [**clear** *low_thresh*]

no threshold ipsec-call-req-rej

no

Deletes the alert or alarm.

high_thresh

Default: 0
Specifies the high threshold number of IPSec call requests rejected per second that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 1000000.

clear *low_thresh*

Default:*0*
Specifies the low threshold number of IPSec call requests rejected per second that must be met or exceeded within the polling interval to clear an alert or alarm.
low_thresh is an integer from 0 through 1000000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of IPSec call requests rejected is equal to or greater than a specified number per second.
Alerts or alarms are triggered for the number of IPSec IKE requests on the following rules:

- **Enter condition:** Actual number of IPSec IKE requests is greater than the high threshold.
- **Clear condition:** Actual number of IPSec IKE requests is less than the low threshold.

Example

The following command configures a number of IPSec call requests rejected threshold of *1000* and a low threshold of *800* for a system using the Alarm thresholding model:

```
threshold ipsec-call-req-rej 1000 clear 800
```

threshold ipsec-ike-failrate

Configures a threshold for the percentage of IPSec IKE failures.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
threshold  ipsec-ike-failrate high_thresh [  clear low_thresh ]

no threshold ipsec-ike-failrate
```

no

Deletes the alert or alarm.

high_thresh

Default: 0
Specifies the high threshold percentage of IPSec IKE failures per second that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 100.

clear *low_thresh*

Default: *0*
Specifies the low threshold percentage of IPSec IKE failures per second that must be met or exceeded within the polling interval to clear an alert or alarm.
low_thresh is an integer from 0 through 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the percentage of IPSec IKE failures is equal to or greater than a specified number per second.
Alerts or alarms are triggered for the percentage of IPSec IKE failures on the following rules:

- **Enter condition:** Percentage of IPSec IKE failures is greater than the high threshold.
- **Clear condition:** Percentage of IPSec IKE failures is less than the low threshold.

Example

The following command configures a percentage of IPSec IKE failures threshold of *1000* and a low threshold of *800* for a system using the Alarm thresholding model:

```
threshold ipsec-ike-failrate 90 clear 80
```

threshold ipsec-ike-failures

Configures a threshold for the total IPSec IKE failures.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

threshold ipsec-ike-failures *high_thresh* [**clear** *low_thresh*]

no threshold ipsec-ike-failures

no

Deletes the alert or alarm.

high_thresh

Default: *0*
Specifies the high threshold number of IPSec IKE failures per second that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 1000000.

clear *low_thresh*

Default:0
Specifies the low threshold number of call IPSec IKE failures per second that must be met or exceeded within the polling interval to clear an alert or alarm.
low_thresh is an integer from 0 through 1000000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of IPSec IKE failures is equal to or greater than a specified number per second.
Alerts or alarms are triggered for the number of IPSec IKE failures on the following rules:

- **Enter condition:** Actual number of IPSec IKE failures is greater than the high threshold.
- **Clear condition:** Actual number of IPSec IKE failures is less than the low threshold.

Example

The following command configures a number of IPSec IKE failures threshold of *1000* and a low threshold of *800* for a system using the Alarm thresholding model:

```
threshold ipsec-ike-failures 1000 clear 800
```

threshold ipsec-ike-requests

Configures a threshold for the total IPSec IKE requests.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
threshold ipsec-ike-requests high_thresh [ clear low_thresh ]

no threshold ipsec-ike-requests
```

no

Deletes the alert or alarm.

high_thresh

Default: 0
Specifies the high threshold number of IPSec IKE requests per second that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 1000000.

clear *low_thresh*

Default:0
Specifies the low threshold number of call IPSec IKE requests per second that must be met or exceeded within the polling interval to clear an alert or alarm.
low_thresh is an integer from 0 through 1000000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of IPSec IKE requests is equal to or greater than a specified number per second.
Alerts or alarms are triggered for the number of IPSec IKE requests on the following rules:

- **Enter condition:** Actual number of IPSec IKE failures is greater than the high threshold.
- **Clear condition:** Actual number of IPSec IKE failures is less than the low threshold.

Example

The following command configures a number of IPSec IKE requests threshold of *1000* and a low threshold of *800* for a system using the Alarm thresholding model:

```
threshold ipsec-ike-requests 1000 clear 800
```

threshold ipsec-tunnels-established

Configures a threshold for the total IPSec tunnels established.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

threshold ipsec-tunnels-established *high_thresh* [**clear** *low_thresh*]

no threshold ipsec-tunnels-established

no

Deletes the alert or alarm.

high_thresh

Default: 0
Specifies the high threshold number of IPSec tunnels established per second that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 1000000.

clear *low_thresh*

Default:0
Specifies the low threshold number of call IPSec tunnels established per second that must be met or exceeded within the polling interval to clear an alert or alarm.
low_thresh is an integer from 0 through 1000000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of IPSec tunnels established is equal to or greater than a specified number per second.
Alerts or alarms are triggered for the number of IPSec tunnels established on the following rules:

- **Enter condition:** Actual number of IPSec tunnels established is greater than the high threshold.
- **Clear condition:** Actual number of IPSec tunnels established is less than the low threshold.

Example

The following command configures a number of IPSec tunnels established threshold of *1000* and a low threshold of *800* for a system using the Alarm thresholding model:

```
threshold ipsec-tunnels-established 1000 clear 800
```

threshold ipsec-tunnels-setup

Configures a threshold for the total IPSec tunnels setup.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
threshold ipsec-tunnels-setup high_thresh [ clear low_thresh  ]

no threshold ipsec-tunnels-setup
```

no

Deletes the alert or alarm.

high_thresh

Default: 0
Specifies the high threshold number of IPSec tunnels setup per second that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 1000000.

clear *low_thresh*

Default:0
Specifies the low threshold number of call IPSec tunnels setup per second that must be met or exceeded within the polling interval to clear an alert or alarm.
low_thresh is an integer from 0 through 1000000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of IPSec tunnels setup is equal to or greater than a specified number per second.
Alerts or alarms are triggered for the number of IPSec tunnels setup on the following rules:

- **Enter condition:** Actual number of IPSec tunnels setup is greater than the high threshold.
- **Clear condition:** Actual number of IPSec tunnels setup is less than the low threshold.

Example

The following command configures a number of IPSec tunnels setup threshold of *1000* and a low threshold of *800* for a system using the Alarm thresholding model:

```
threshold ipsec-tunnels-setup 1000 clear 800
```

threshold reg-reply-error

Set an alarm or alert based on the number of registration reply errors per HA service.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

threshold reg-reply-error *high_thresh* [**clear** *low_thresh*]

no threshold reg-reply-error

no

Deletes the alert or alarm.

high_thresh

Default: 0
Specifies the high threshold number of registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 100000.

clear *low_thresh*

Default:0
Specifies the low threshold number of registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. *low_thresh* is an integer from 0 through 100000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of registration reply errors is equal to or greater than a specified number of calls per second.
Alerts or alarms are triggered for the number of registration reply errors on the following rules:

- **Enter condition:** Actual number of registration reply errors is greater than the high threshold.
- **Clear condition:** Actual number of registration reply errors is less than the low threshold.

Example

The following command configures a registration reply error threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold reg-reply-error 1000 clear 500
```

threshold rereg-reply-error

Set an alarm or alert based on the number of re-registration reply errors per HA service.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

threshold rereg-reply-error *high_thresh* [**clear** *low_thresh*]

no threshold rereg-reply-error

no

Deletes the alert or alarm.

high_thresh

Default: 0
Specifies the high threshold number of re-registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 100000.

clear *low_thresh*

Default:0
Specifies the low threshold number of re-registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. *low_thresh* is an integer from 0 through 100000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of re-registration reply errors is equal to or greater than a specified number of calls per second.
Alerts or alarms are triggered for the number of re-registration reply errors on the following rules:

- **Enter condition:** Actual number of re-registration reply errors is greater than the high threshold.
- **Clear condition:** Actual number of re-registration reply errors is less than the low threshold.

Example

The following command configures a reregistration reply error threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold dereg-reply-error 1000 clear 500
```

wimax-3gpp2 interworking

Configures the interworking between WiMAX and 3GPP2 network at HA. This support provides handoff capabilities from 4G to 3G (PDSN) network access and vice-versa.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
[no | default] wimax-3gpp2 interworking
```

no

Disables the pre-configured interworking between WiMAX and 3GPP2 networks at HA level.

default

Configures the **WiMAX-3GPP2 interworking** to default setting: disabled.

Usage

Use this command to enable/disable the interworking between WiMAX and 3GPP2 network for seamless session continuity.
This functionality provides HA support for both 4G and 3G technology HA (WiMAX HA and PDSN/HA) for handoff from 4G and 3G network access (ASN GW/FA and PDSN/FA) and vice-versa.

Important: Use this command in conjunction with the **authentication aaa-distributed-mip-keys required** command.

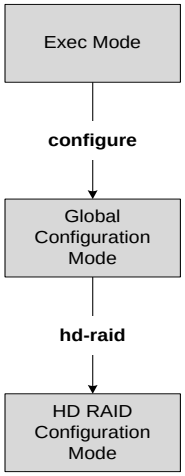
Example

The following command enables the interworking for a subscriber between WiMAX and 3GPP2 network.

```
wimax-3gpp2 interworking
```

Chapter 141
HD RAID Configuration Mode Commands

This mode develops default policies designed to minimize administrative intervention when setting up the RAID on ASR 5000 SMC hard disks.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

overwrite

Sets the RAID overwrite properties.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] overwrite { invalid | unknown | valid } disk [ -noconfirm ]
```

no

Prevents a disk from being overwritten.

default

Configures the default overwrite action:

invalid

This option allows the system to automatically overwrite invalid disks including empty disks, wrongly partitioned disks, and partially constructed disks.
This is the default overwrite action.

unknown

This option allows the system to automatically overwrite unknown disks that has a valid RAID superblock but is not configured in the standard way; most likely because it has data from a different version.

valid

This option allows the system to automatically overwrite a disk that is a clean RAID component but not part of the current or selected RAID.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Sets a policy for automatically overwriting different disk types. If there is a disk that satisfies the changed overwrite policy then the disk would overwrite immediately.

Example

The following command configures a policy for overwriting invalid RAID disks:

```
overwrite invalid disk -noconfirm
```

select

Configures the disk preference when both hard disks on the ASR 5000 have valid RAID information.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ default ] select { newer | none } disk [ -noconfirm ]
```

default

Configures the command to its default condition.

newer

Selects the newer disk by timestamp and event counter in superblocks. If all are the same, then the same array will start with both SMC disks, but a different array will need admin intervention).

none

Does not select any disk but defers to administrator intervention.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Determines the selected disc when two valid disks from either the same or different RAIDs are running on the ASR 5000.

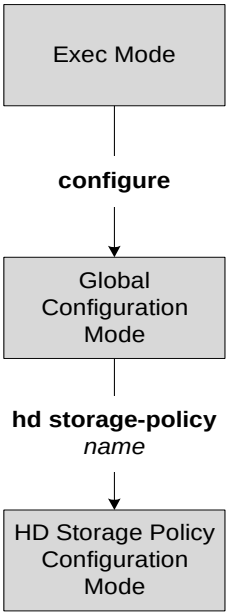
Example

This command forces the RAID to be configured on the newer SMC hard disk:

```
select newer disk -noconfirm
```

Chapter 142
HD Storage Policy Configuration Mode Commands

The HD Storage Policy Configuration Mode is used to configure directory name and file parameters for Diameter record files being stored on the HD storage device.



directory

Configures the name of the directory on the HD storage drive where Diameter records are stored.

Product

HSGW, P-GW, S-GW

Privilege

Administrator

Syntax

directory name *dir_name*

default directory name

default

Returns the command to its default setting of using the policy name as the directory name.

name *dir_name*

Specifies the name to be applied to the directory. *dir_name* must be an alphanumeric string of 1 through 63 characters.
When configured, the actual directory path is:

```
/hd-raid/records/<record-type>/<dir_name>/
```

So if the directory name variable is entered as "*sgwpgw*", the path is:

```
/hd-raid/records/acr/sgwpgw
```

Usage

Use this command to name a directory on the HD storage drive where Diameter records are to be stored.

Example

The following command configures a directory named *cdr1*:

```
directory name cdr1
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

file

Configures file parameters for Diameter records being stored on the HD storage device.

Product

HSGW, P-GW, S-GW

Privilege

Administrator

Syntax

```
file { format acr { custom1...custom10 } | name { extension string | prefix string } |
rotation { record-count num | time-interval sec | volume mb mbytes } }

default file { format acr | name prefix | rotation { record-count | time-interval |
volume } }

no file ( extension | rotation { record-count | time-interval } }
```

default

Returns the command to the default settings for the specified keywords.

no

Removes the configuration for the specified parameters.

format acr { custom1...custom10 }

Default: **custom1**
Specifies the file format used when storing records on the HD storage device. **custom1** is a vendor-specific file format.

name { extension *string* **| prefix** *string* **}**

Specifies a string to be pre-pended or appended to the filenames. By default, the policy name is used for the prefix.
extension *string*: Specifies a file extension to append to the filename. *string* must be an alphanumeric string of 1 through 10 characters.
prefix *string*: Specifies a file prefix to append to the filename. *string* must be an alphanumeric string of 1 through 63 characters. This parameter replaces the policy name used by default.

rotation { record-count *num* **| time-interval** *sec* **| volume mb** *mbytes* **}**

Specifies the triggers that prompt file rotation on the HD storage drive. All options can be configured and upon reaching any of the thresholds, file rotation is initiated.
record-count *num*: File rotation occurs when the number of records reaches the number configured in this keyword. *num* must be an integer from 1000 through 65000. Default = 10000
time-interval *sec*: File rotation occurs at time intervals (in seconds) configured by this keyword. *sec* must be an integer from 30 through 86400. Default = 3600 (1 hour)
volume mb *mbytes*: File rotation occurs when the record volume exceeds the value (in megabytes) configured by this keyword. *mbytes* must be an integer from 2 through 40. Default = 4

Usage

Use this command to configure file parameters for Diameter records being stored on the HD storage device.

Example

The following command sets the file rotation thresholds for files being stored on the HD storage device:

```
file rotation volume mb 4

file rotation record-count 15000

file rotation time-interval 7200
```

The following command replaces the policy name as the prefix of all files being stored through this policy with the prefix *sgw*:

```
file name prefix sgw
```

Chapter 143
HLR Configuration Mode Commands

The HLR Configuration Mode provides the commands and parameters to configure the home location register (HLR) node that is the database containing the subscriber profile and connection information for a specific GPRS/UMTS core network.

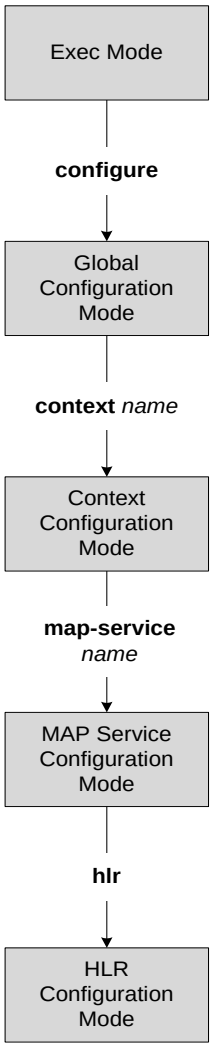
In this mode, your prompt will look similar to:

```
[<context_name>]hostname(config-map-service-<svr_name>-hlr)#
```

The HLR Configuration Mode is a sub-mode derived from the MAP Configuration Mode which controls the MAP service configuration. It is the MAP service that provides the application-layer protocol support used to connect the HLR to other nodes in the network such as the SGSN.

When the mode is accessed, the command line will appear similar to

```
[<ctx_name>]asr5000(config-map-service-<service_name>-hlr)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

acn-version-retention

This command configures the ACN version retention method.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
acn-version-retention { per-imsi-prefix | per-subscriber }

default acn-version-retention
```

default

Returns the configuration to the default value: retains the version information per IMSI prefix.

per-imsi-prefix

Retain ACN version information, for communication with the HLR, on a per IMSI prefix basis.

per-subscriber

Retain ACN version information, for communication with the HLR, on a per buscriber basis.

Usage

By default, the SGSN sends ACN version 3 SAI (service area identity) to the HLR. If the SGSN receives an error message indicating that the HLR does not support that version, then the SGSN tries again with an ACN version 2 SAI. Next time the SGSN communicates with that HLR, it retains that version information and version persists based on the IMSI prefix.
Use this command to enable the SGSN to retain version according to subscriber.

Example

Configure the SGSN to retain version information according to the IMSI prefix:

```
default acn-version-retention
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Return to the Exec mode.

exit

Exits the current configuration mode and returns to the MAP Service configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the MAP Service configuration mode.

imsi

This command sets up IMSI (International Mobile Subscriber Identity) -based configuration. The IMSI prefix includes the nobile country code (MCC) and the mobile network code (MNC).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] imsi { any | starts-with *prefix_number* **} { imsi [sgsn-source-address-format point-code-ssn [source-ssn** *ssn* **] | isdn** *isdn_number* **| mobile-global-title** *mgt_number* **[max-gt-address-len** *max_gt_address* **] | point-code** *pt-code* **} }**

no

Removes the imsi-prefix definition from the configuration.

any

Configures acceptance of any IMSI prefix.

start-with *prefix_number*

Selects IMSI prefix-based routing.
prefix_number is a string of up to 15 integers.

imsi

Enables configurable default behavior for routing.
Entering **imsi** with the **any** keyword preserves the default behavior and the E.212 address is used as a destination address and the MAP request will be sent towards the HLR.
If this keyword is not used with the **any** keyword, then the MAP request will be rejected.

isdn *isdn_number*

Defines the E.164 number of the HLR.
isdn_number is a string of integers, up to 15.

mobile-global-title *mgt_number* **[max-gt-address-len** *max_gt_address_length* **]**

Defines the mobile global title address that the MCC/MNC portion of the IMSI will be converted to. If the maximum GT address length is specified (optional) and if the length of the MGT string is greater than defined, then the least significant digits will be omitted.
mgt_number is a string of digits, up to 18 digits in length.
max_gt_address is an integer from 1 to 32.

point-code *pt-code* **source-ssn** *ssn*

Defines the point code for the HLR.
pt-code is a string of digits, up to 11; SS7 format preferred.

sgsn-source-address-format point-code-ssn

Selects HLR call process according to SCCP calling party address of the SGSN. This will be filled at MAP level, including the ITU point code address.

source-ssn *ssn*

Defines the SSN of the source that will be used for the call filtering.
ssn: Must be an integer from 1 to 255.

Usage

Routing will be done according to IMSI parameters configured with this command or according to the mobile global title address (replacing the MCC/MNC portion of the IMSI) is so specified.

Example

```
imsi starts-with 3 isdn 123456789 sgsn-source-address-form at point-code-ssn
```

policy routing

This command configures the policy for the routing of MAP messages. If this command is not configured or disabled (with the **default** keyword), then routing is done according to the configuration of the IMSI parameters.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
policy routing { hlr-isdn | ms-isdn }

default policy routing

no policy routing
```

default

Resets the policy routing to the system default, disabled.

no

Removes the policy routing configuration from the system.

hlr-isdn

Selects HLR-ISDN based routing.

ms-isdn

Selects mobile station (MS)-ISDN based routing.

Usage

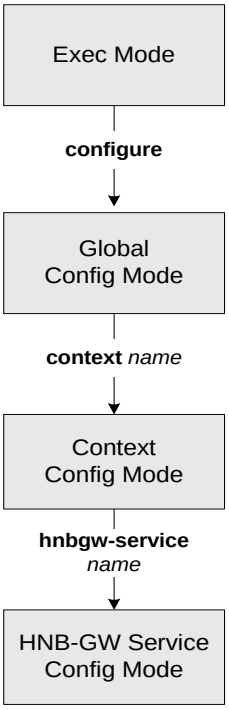
Use this command to set the policy for routing MAP messages.

Example

```
policy routing hlr-isdn
```

Chapter 144
HNB-GW Service Configuration Mode Commands

The 3G UMTS Home-NodeB Gateway Service Configuration Mode manages access to the UMTS core network in a 3G UMTS network through a Femto node.



access-control-db

Configures the access control database parameters in an HNB-GW service instance to control HNB and UE access to the HNB-GW node.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

```
access-control-db imsi-purge-timeout {immidiate | dur }

default access-control-db imsi-purge-timeout
```

default

Sets the default value to HNB-UE access control database on HNB-GW service instance.
The default timeout duration for purging of the IMSI White List from the HNB-GW Access Control database is 24 hours. The HNB-GW service waits for 24 hours after all referenced HNBs have de-registered before purging the records.

immidiate

Sets the HNB-GW service to purge the HNB-UE access control database immediately after all referenced HNBs have de-registered.

imsi-purge-timeout *dur*

Sets the timeout duration (in minutes) for the access control database to wait before purging the IMSI values received as a White List from HMS/BAC.
After all HNBs have de-registered, the Access Control database on HNB-GW maintains the IMSI White List received from HMS/BAC during HNB registration procedure for the configured durations before purging the list.
dur is an integer from 1 through 1440.

Usage

Use this command to configure the HNB-UE access control database parameters on HNB-GW service.
This command sets the timeout duration to maintain the IMSI White List received from HMS/BAC during HNB registration procedure in HNB-GW service for the configured *dur* in minutes after de-registration of all referenced HNBs from HNB-GW node and then purge the database.

Example

Following command sets the HNB-GW service instance to purge all IMSI records from HNB-UE access control database immediately after all referenced HNBs de-registered from HNB-GW service instance.

```
access-control-db imsi-purge-timeout immidiate
```

associate gtpu-service

Associates a previously configured GTP-U service to bind the HNB-GW service with an HNB towards the HNB side. A GTP-U service must be configured in Context Configuration mode before using this configuration.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

associate gtpu-service *svc_name*

no associate gtpu-service

no

Removes the associated GTP-U service from this HNB-GW service configuration.

svc_name

Identifies the name of the pre-configured GTP-U service to associate with an HNB-GW service towards the Home-NodeB side.
svc_name ise an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure GTP-U data plan between HNB-GW service and Home-NodeB. The service defined for GTP-U can be configured in Context configuration mode.

Important: Another GTP-U service can be used to bind the HNB-GW service towards the Core Network and can be configured in HNB-PS Configuration mode. For more information on GTP-U service configuration, refer *GTP-U Service Configuration Mode Commands*.

Example

Following command associates GTP-U service named *gtpu-hnb1* with specific HNB-GW service towards Home-NodeB side.

```
associate gtpu-service gtpu-hnb1
```

associate rtp pool

Associates a previously defined RTP pool (IP pool) with the HNB-GW service. This pool is used by HNB-GW to send an IP address to HNB where HNB uses it to map the RTP streams over Iuh interface. This command is used for RTP stream management on HNB-GW.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

associate rtp pool *pool_name*

no associate rtp pool

no

Removes the associated RTP pool (IP pool) from this HNB-GW service configuration.

pool_name

Specifies the name of the pre-configured RTP IP pool that the HNB-GW uses to assign IP addresses when mapping RTP streams over the Iuh interface.
pool_name is an alphanumeric string of 1 through 31 characters.

Important: For IP pool (RTP pool) configuration, refer **ip pool** command in *Context Configuration Mode Commands* chapter.

Usage

Use this command to associate an RTP pool (IP Pool) with an HNB-GW service for allotment of RTP IP address to HNB-GW node and send the same to HNB for RTP stream management support. The HNB maps the RTP streams with received IP address(es) while communicating with HNB-GW over Iuh interface where HNB-GW communicates with MSC/VLR through IuCS-over-IP tunnel.
This command is used for RTP stream management on HNB-GW.

Important: This command must be used to provide IP address for mapping of RTP streams on Iuh interface between HNB and HNB-GW.

Example

Following command associates RTP pool named *rtp_1* with HNB-GW service for RTP stream end point from Home-NodeB:

```
associate rtp pool rtp_1
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

handin

Allows or disallows the incoming hand-over of an MS in HNB-GW via the Serving Radio Network Subsystem (SRNS) Relocation procedure for the specified packet switched/circuit switched (PS/CS) core network (CN) domain.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

```
[no | default] handin cn-domain [cs | ps]
```

no

Disallows the incoming MS hand-over for the particular CN domain via SRNS Relocation procedure in an HNB-GW service instance.
If hand-over is restricted the relocation request will be rejected with rejection cause “Relocation Not Supported In Target RNC Or Target System”.

default

Sets the HNB-GW service instance to allow the incoming MS hand-over for the particular CN domain via SRNS Relocation procedure in an HNB-GW service instance.

cs

Sets the HNB-GW service instance to allow the incoming MS hand-over for the CS core network domain via SRNS Relocation procedure in an HNB-GW service instance.

ps

Sets the HNB-GW service instance to allow the incoming MS hand-over for the PS core network domain via SRNS Relocation procedure in an HNB-GW service instance.

Usage

Use this command to set HNB-GW service instance for allowing/disallowing incoming hand-over of an MS in HNB-GW via SRNS Relocation procedure for PS or CS core network domain.
If hand-over is restricted the Relocation Request message will be rejected with rejection cause “Relocation Not Supported In Target RNC Or Target System”.

Example

The following command configures the HNB-GW service instance to allow hand-over of an MS in HNB-W via SRNS Relocation procedure for PS core network domain:

```
handin ps
```

hnb-access-mode

Configures the HNB access mode (open/closed) in HNB-GW service instance and related parameters. Currently it is used to configured Open Access mode support only.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

hnb-access-mode open max-registered-ue *reg_ue*

no hnb-access-mode open

default hnb-access-mode open

no

Disables Open Access mode support.
If disabled and an Open HNB tries to register, the HNB-GW sends HNB-Registration-Reject message with "OA&M Intervention" cause.

Important: UE-Reg/CS-Call/PS-Call requests (both existing and future) is allowed from already registered Open HNBs even after operator has disabled the Open Access support. No new Open HNB registration is allowed once operator disables the Open Access support.

default

Sets the default configuration of Open Access mode support.
By default, HNB-GW allows registration of Open HNBs and a maximum of 16 UEs can register from an open HNB in an HNB-GW service instance.

open max-registered-ue *reg_ue*

Sets the HNB-GW service instance to allow the maximum number of UEs through an open HNB under Open Access mode support.
reg_ue defines the maximum number of UEs that can register from an Open HNB as an integer from 1 through 32.
If a UE tries to register from an Open HNB which has already reached to the configured limit configured, the HNB-GW sends HNB-Registration-Reject message with "ue not allowed in this hnb" cause in an HNB-GW service instance.

Usage

Use this command to configure the HNB-GW service instance for Open Access Mode support and related parameters.
This command enable Open Access mode support to allow the UEs that can register from an Open HNB. If a UE tries to register from an Open HNB with an HNB-GW service instance, which is already reached to the limit configured through **max-registered-ue** *reg_ue* the HNB-GW sends HNB-Registration-Reject message with "*ue not allowed in this hnb*" cause.

Important: If Operator has reduced the maximum number of UEs allowed per Open HNB during the session, this will not have any effect on already registered UEs/CS-Calls/PS-Calls even if previously configured *reg_ue* is beyond the newly configured *reg_ue* value. Limits is respected while handling new requests.

Example

The following command configures the HNB-GW service instance to allow 16 UEs to register through an open HNB:

```
default hnb-access-mode open
```

ip iu-qos-dscp

Enables or disables the DSCP marking parameter for data packets carried over over an IuCS/IuPS interface towards MSC/SGSN. By default this command is **Disabled**.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

ip iu-qos-dscp protocol { **sctp payload all** | **udp payload** { **gtpu** | **rtcp**| **rtp**} } *dscp_code*

[**default** | **no**] **ip iu-qos-dscp protocol** { **sctp payload all** | **udp payload** { **gtpu** | **rtcp**| **rtp**} }

no

Use this keyword to place the configuration in **pass-through** mode (no marking of DSCP). Use of this keyword is allowed even when there is no previous DSCP parameter set.

Important: In this configuration the **no** keyword does not disable or remove a previous configuration.

default

Enables the DSCP marking on HNB-GW and set/restores the QoS parameters to their default setting.

sctp payload all *dscp_code*

Specifies the QoS traffic pattern towards MSC/SGSN in SCTP protocol association over IuCS/IuPS interface. By this keyword the Traffic classes specified by a user based on SCTP protocol and all type of payload identified based on the transport level port numbers.
By default DSCP codes **cs5** is supported for **all** payloads in SCTP protocol.

udp payload { gtpu | rtcp| rtp} *dscp_code*

Specifies the QoS traffic pattern towards MSC/SGSN in SCTP protocol association over IuCS/IuPS interface. By this keyword the Traffic classes specified by a user based on UDP protocol and GTPU, RTCP, and RTP type of payload identified based on the transport level port numbers.
Default DSCP code in UDP traffic are:

- **GTP-U**: cs1
- **RTCP**: ef
- **RTP**: af41

dscp_code

Specifies the QoS DSCP codes supported for SCTP and UDP traffic and its payloads towards MSC/SGSN over IuCS/IuPS interface.
following type of DSCP codes *dscp_code* are supported over IuH interface:

- **af11**: Marks traffic as Assured Forwarding 11 PHB (high throughput data)
- **af12**: Marks traffic as Assured Forwarding 12 PHB (high throughput data)
- **af13**: Marks traffic as Assured Forwarding 13 PHB (high throughput data)
- **af21**: Marks traffic as Assured Forwarding 21 PHB (low latency data)
- **af22**: Marks traffic as Assured Forwarding 22 PHB (low latency data)
- **af23**: Marks traffic as Assured Forwarding 23 PHB (low latency data)
- **af31**: Marks traffic as Assured Forwarding 31 PHB (multimedia streaming)
- **af32**: Marks traffic as Assured Forwarding 32 PHB (multimedia streaming)
- **af33**: Marks traffic as Assured Forwarding 33 PHB (multimedia streaming)
- **af41**: Marks traffic as Assured Forwarding 41 PHB (multimedia conferencing). This is the default DSCP code for RTP payloads in UDP protocol.
- **af42**: Marks traffic as Assured Forwarding 42 PHB (multimedia conferencing)
- **af43**: Marks traffic as Assured Forwarding 43 PHB (multimedia conferencing)
- **cs1**: Marks traffic with Class Selector 1 (low priority data). This is the default DSCP code for GTP-U payloads in UDP protocol.
- **cs2**: Marks traffic with Class Selector 2 (OAM)
- **cs3**: Marks traffic with Class Selector 3 (broadcast video)
- **cs4**: Marks traffic with Class Selector 4 (real-time interactive)
- **cs5**: Marks traffic with Class Selector 5 (signaling). This is the default DSCP code for all SCTP payloads.
- **cs6**: Marks traffic with Class Selector 6 (network control)
- **df** : Marks traffic as Default Forwarding (best effort: DSCP = 0)
- **ef**: Marks traffic as Expedited Forwarding PHB (telephony). This is the default DSCP code for RTCP payloads in UDP protocol.

Usage

Use this command to enable/disable the DSCP marking for data packets over IuCS/PS interface. This command assigns the DSCP levels to specific traffic patterns in order to ensure that the packets are delivered according to the precedence with which they are tagged. The Diffserv markings are applied to the IP header of every subscriber data packet transmitted over IuCS/IuPs interface(s) towards MSC/SGSN.
This command adds DSCP marking on egress traffic going towards CN (CS/PS). To make the configuration **pass-through** mode or not marking DSCP at all in the packets, **no** variant of command is used. Use of **no** is allowed even when there is no previous DSCP configuration done.

Important: By default this command is **Disabled**.

Important: When DSCP configuration is not specified, the system works in **pass-through** mode and DSCP values in the ingress (from CN) and egress (to HNB) data packets remain unchanged. Multiple traffic classes can share the same code point value.

Following type shown in following tables respectively:

Table 23. Supported DSCP Codes and Service Class

Service Class	DSCP Code	Service Class	DSCP Code
high throughput data	af11 af12 af13	low priority data	cs1
low latency data	af21 af22 af23	OAM	cs2
multimedia streaming	af31 af32 af33	broadcast video	cs3
multimedia conferencing	af41 af42 af43	real-time interactive	cs4
best effort/ default forwarding, value zero	df	Signaling	cs5
telephony	ef	network control	cs6

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

Example

The following command configures the DSCP code for the SCTP IuCS/IuPS streaming traffic pattern for all payloads to be **ef**:

```
ip iu-qos-dscp protocol sctp payload all ef
```

ip iuh-qos-dscp

Enables or disables the DSCP marking parameter for control and data packets transmitted over an IuH interface towards HNB. By default this command is **Disabled**.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

ip iuh-qos-dscp protocol { **sctp payload all** | **udp payload** { **gtpu** | **rtcp**| **rtp**} } *dscp_code*

[**default** | **no**] **ip iuh-qos-dscp protocol** { **sctp payload all** | **udp payload** { **gtpu** | **rtcp**| **rtp**} }

no

Use this keyword to set the configuration in **pass-through** mode. Use of this keyword is allowed even when there is no previous DSCP parameter set.

Important: In this configuration the **no** keyword does not disable/remove a previous configuration.

default

Enables the DSCP marking on HNB-GW and set/restores the QoS parameters to its default setting.

sctp payload all *dscp_code*

Specifies the QOS traffic pattern towards HNB in SCTP protocol association over IuH interface.
By this keyword the Traffic classes specified by a user based on SCTP protocol and all type of payload identified based on the transport level port numbers.
By default DSCP codes **cs5** is supported for **all** payloads in SCTP protocol.

udp payload { gtpu | rtcp| rtp} *dscp_code*

Specifies the QOS traffic pattern towards HNB in SCTP protocol association over IuH interface.
By this keyword the Traffic classes specified by a user based on UDP protocol and GTPU, RTCP, and RTP type of payload identified based on the transport level port numbers.
Default DSCP code in UDP traffic are:

- **GTP-U**: cs1
- **RTCP**: ef
- **RTP**: af41

dscp_code

Specifies the QOS DSCP codes supported for SCTP and UDP traffic and its payloads towards HNB over IuH interface.
following type of DSCP codes *dscp_code* are supported over IuH interface:

- **af11**: Marks traffic as Assured Forwarding 11 PHB (high throughput data)
- **af12**: Marks traffic as Assured Forwarding 12 PHB (high throughput data)
- **af13**: Marks traffic as Assured Forwarding 13 PHB (high throughput data)
- **af21**: Marks traffic as Assured Forwarding 21 PHB (low latency data)
- **af22**: Marks traffic as Assured Forwarding 22 PHB (low latency data)
- **af23**: Marks traffic as Assured Forwarding 23 PHB (low latency data)
- **af31**: Marks traffic as Assured Forwarding 31 PHB (multimedia streaming)
- **af32**: Marks traffic as Assured Forwarding 32 PHB (multimedia streaming)
- **af33**: Marks traffic as Assured Forwarding 33 PHB (multimedia streaming)
- **af41**: Marks traffic as Assured Forwarding 41 PHB (multimedia conferencing). This is the default DSCP code for RTP payloads in UDP protocol.
- **af42**: Marks traffic as Assured Forwarding 42 PHB (multimedia conferencing)
- **af43**: Marks traffic as Assured Forwarding 43 PHB (multimedia conferencing)
- **cs1**: Marks traffic with Class Selector 1 (low priority data). This is the default DSCP code for GTP-U payloads in UDP protocol.
- **cs2**: Marks traffic with Class Selector 2 (OAM)
- **cs3**: Marks traffic with Class Selector 3 (broadcast video)
- **cs4**: Marks traffic with Class Selector 4 (real-time interactive)
- **cs5**: Marks traffic with Class Selector 5 (signaling). This is the default DSCP code for all SCTP payloads.
- **cs6**: Marks traffic with Class Selector 6 (network control)
- **df** : Marks traffic as Default Forwarding (best effort: DSCP = 0)
- **ef**: Marks traffic as Expedited Forwarding PHB (telephony). This is the default DSCP code for RTCP payloads in UDP protocol.

Usage

Use this command to enable/disable the DSCP marking for control and data packets carried by the IP protocols and their payloads on IuH. This command assigns the DSCP levels to specific traffic patterns in order to ensure that the packets are delivered according to the precedence with which they are tagged. The Diffserv markings are applied to the IP header of every subscriber data packet transmitted over IuH interface(s) towards HNB.

This command adds DSCP marking on egress traffic going towards HNB. To make the configuration **pass-through mode** or not marking DSCP at all in the packets, **no** variant of command is used. Use of **no** is allowed even when there is no previous DSCP configuration done.

Important: By default this command is **Disabled**.

Important: When DSCP configuration is not specified, system works in **pass-through** mode and DSCP value in the ingress (from CN) and egress (to HNB) control and data packets remain unchanged. Multiple traffic classes can share the same code point value.

Following type shown in following tables respectively:

Table 24. Supported DSCP Codes and Service Class

Service Class	DSCP Code	Service Class	DSCP Code
high throughput data	af11 af12 af13	low priority data	cs1
low latency data	af21 af22 af23	OAM	cs2
multimedia streaming	af31 af32 af33	broadcast video	cs3
multimedia conferencing	af41 af42 af43	real-time interactive	cs4
best effort/ default forwarding, value zero	df	Signaling	cs5
telephony	ef	network control	cs6

Example

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

The following command configures the DSCP code for the SCTP IuH streaming traffic pattern for all payloads to be **ef**:

```
ip iuh-qos-dscp protocol sctp payload all ef
```

paging open-hnb

Cconfigures paging optimization parameters for open HNBs connected through Open Access mode in the HNB-GW service instance. Currently it is used to configure paging optimization for Open Access mode support only.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

paging open-hnb [**hnb-where-ue-registered fallback**] {**always** | **never** | **only-if-with-paging-area**}

default paging open-hnb

default

Sets the default behavior of paging optimization configuration for an open HNB while using Open Access mode support.
By default the HNB-GW pages open HNBs only if paging-area IE is received in the paging message.

{always | never | only-if-with-paging-area}

Sets the HNB-GW service instance to page open HNB for a paging message.
always: Sets the system to ALWAYS page the open HNBs irrespective of **paging-area** IE is received in paging messages.
never: Sets the system to NEVER page any open HNB.
only-if-with-paging-area: Sets the system to page the open HNBs only when **paging-area** IE is received in paging messages.

hnb-where-ue-registered fallback {always | never | only-if-with-paging-area}

Sets the HNB-GW service instance to page open HNB from where the UE is registered.
always: Sets the system to ALWAYS page the open HNBs from where the UE is registered. If the UE is not registered then it pages the open HNBs irrespective of **paging-area** IE is received in paging messages.
never: Sets the system to page the open HNBs from where the UE is registered. If the UE is not registered then it NEVER pages any open HNB.
only-if-with-paging-area: Sets the system to ALWAYS page the open HNBs from where the UE is registered. If the UE is not registered then it pages the open HNBs only when **paging-area** IE is received in paging messages.

Usage

Use this command to configure the paging optimization parameters for open HNBs connected through Open Access mode in HNB-GW service instance.

Example

The following command configures the HNB-GW service instance to page an open HNB from where the UE is connected and paging-area IE is received in paging message:

```
paging open-hnb hnb-where-ue-registered fallback only-if-with-paging-area
```

radio-network-plmn

Creates, remove and enters the HNB-RN-PLMN Configuration mode. In this mode you can configure various parameters for radio network public mobile land networks (PLMNs). A maximum of 16 radio PLMN-IDs can be configured in an HNB-GW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

radio-network-plmn mcc *mcc_num* **mnc** *mnc_num* [**-noconfirm**]

no radio-network-plmn mcc *mcc_num* **mnc** *mnc_num*

no

Removes the configured radio network PLMN identifier for an HNB-GW service.

Caution: Removing the PLMN-ID is a disruptive operation; the HNB-GW service will be re-started.

mcc *mcc_num*

Specifies the mobile country code (MCC) part of radio network PLMN identifier as an integer value from 101 through 998.

mnc *mnc_num*

Specifies the mobile network code (MNC) part of radio network PLMN identifier as a 2- or 3-digit integer from 01 through 998.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to configure the radio network PLMN identifier for an HNB-GW service. This command also creates a configuration mode to configure various parameters for defined radio network PLMN identifier in HNB-GW service.

Caution: Changing or removing the PLMN-ID is a disruptive operation; the HNB-GW service will be re-started.

Entering this command results in the following prompt:

```
[context_name]hostname(config-radio-network-plmn)#
```

A maximum of 16 radio network PLMN identifiers are supported for an HNB-GW service.

Example

The following command configures the radio network PLMN identifier with MCC value as *102* and MNC value as *20* for an HNB-GW service:

```
radio-network-plmn mmc 102 mnc 20
```

ranap reset

Configures various Radio Access Network (RAN) Application Part reset procedure parameters in an HNB access network.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

ranap reset {**ack-timeout** *timer_value* | **guard-timeout** *g_timer* | **hnbgw-initiated** | **max-retransmissions** *retries*}

default ranap reset {**ack-timeout** | **guard-timeout** | **hnbgw-initiated** | **max-retransmissions**}

no ranap hnbgw-initiated

default

Resets the RANAP RESET parameters on HNB-GW service instance.

no

Disables the RANAP RESET procedure related parameters in an HNB-GW service instance.

ack-timeout *timer_value*

Sets the timer value (in seconds) to wait for Reset Acknowledge from SGSN/MSC. This is used during HNB-GW initiated RANAP RESET procedure in HNB-GW service instance.
timer_value is an integer value from 5 through 10. Default: 10

guard-timeout *g_timer_value*

Sets the timer value (in seconds) to send Reset Acknowledge to SGSN/MSC. After this duration the HNB-GW sends RESET-ACK to SGSN/MSC. This is used during SGSN/MSC initiated RANAP RESET procedure in HNB-GW service instance.
g_timer_value is an integer value from 5 through 10. Default: 10

hnbgw-initiated

Enables the HNB-GW Initiated RANAP RESET procedures. Default: Disabled

max-retransmission *retries*

Sets the maximum number of retires allowed for transmission of RESET-ACK message to SGSN/MSC. This is used during RANAP RESET procedure in HNB-GW service instance.
retries is an integer value from 0 through 2. When 0 is used retransmission is disabled. Default: 1

Usage

Use this command to configure the RANAP RESET procedure related parameters in HNB-GW service.

Example

The following command configures the HNB-GW initiated RANAP RESET Procedure for an HNB-GW service:

```
ranap reset hnbgw-initiated
```

rtcp report

Enables or disables the generation of RTP Control Protocol (RTCP) packet/report types on a per HNB-GW service instance basis. It also sets the time interval in seconds between two consecutive RTCP reports.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

```
rtcp report interval dur

[no | default] rtcp report interval
```

no

Disables the RTCP report generation on HNB-GW service. When RTP configuration is not explicitly mentioned, this is the default behavior.

default

Restores the report interval value to its default value of 5 seconds.

interval *dur*

Sets the time interval (in seconds) between two consecutive RTCP reports as an integer from 5 through 30. Default: 5

Usage

Use this command to configure the enabling or disabling of the generation of RTCP packet/ report types on a per HNB-GW service instance basis and sets the specified time interval in seconds between two consecutive RTCP reports.

RTCP enables the receiver to detect if there is any packet loss and needs to compensate for any delay jitter. RTP and RTCP protocols work independently of the underlying Transport layer and Network layer protocols. Whenever this command is disabled, RTCP report generation stops from the next expiry of the previously configured interval and after enabling, reports are generated only for the calls that established as new calls in the future. For existing calls reports generated as per configuration in place.

RTCP reports are generated for each RAB for RTP received from and sent to IuH interface.

Important: The same interval is applicable for all kinds of RTCP packets/ reports across all sessions on an HNB-GW service.

Example

The following command configures the RTCP report generation interval to *15* seconds on an HNB-GW service for RTP stream:

```
rtcp report interval 15
```

rtp mux

Configures the HNB-GW service to allow an Home-NodeB to multiplex multiple RTP streams in one IP packet. This support is provided for RTP stream management feature on HNB-GW.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

[no | default]rtp mux

default

Sets the multiplexing option to default state of "disabled".

no

Removes the configured option to multiplex multiple RTP stream in one packet by Home-NodeB in HNB-GW configuration.

Usage

Use this command to allow an Home-NodeB to multiplex multiple RTP streams in one IP packet. This configuration support is provided for RTP stream management feature on HNB-GW and it is disabled by default.

Example

The following command sets the HNB-GW to allow HNB to multiplex multiple RTP stream in one packet:

```
rtp mux
```

sctp

Configures the SCTP-related parameters like timeout duration for various timers and cookie life over an IuH interface in an HNB-GW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

sctp alpha-rto *alpha_rto_dur*

sctp beta-rto *beta_rto_dur*

sctp checksum-type [**adler32** | **crc32**]

sctp cookie-life *cookie_life*

sctp max-retx [**init** | **path** | **assoc**] *max_retry*

sctp mtu-size [**start** | **min** | **max**] *mtu_byte*

sctp rto { **initial** *ini_rto_dur* | **min** *min_rto_dur* | **max** *max_rto_dur* }

sctp sack-frequency *sack_frq*

sctp sack-period *sack_dur*

sctp max-in-strms *in_strms*

sctp max-out-strms *out_strms*

default sctp {**alpha-rto** | **beta-rto** | **checksum-type** | **cookie-life** | **max-retx** [**init** | **path** | **assoc**] | **mtu-size** [**start** | **min** | **max**] | **rto** { **initial** | **min** | **max**} | **sack-frequency** | **sack-period** | **max-in-strms** | **max-out-strms** }

default

Restores the SCTP parameters to default value in HNB-GW service instance. Default values for all parameters are as follows:

- **alpha-rto**: 5 seconds
- **beta-rto**: 10 seconds
- **checksum-type**: CRC32
- **cookie-life**: 600 ms
- **max-retx init**: 5 retries
- **max-retx path**: 5 retries
- **max-retx assoc**: 10 retries

- **mtu-size min**: 508 Bytes
- **mtu-size max**: 1500 Bytes
- **mtu-size start**: 508 Bytes
- **rto initial**: 30 seconds
- **rto min**: 10 seconds
- **rto max**: 600 seconds
- **sack-frequency**: 2
- **sack-period**: 2 ms
- **max-in-strms**: 4
- **max-out-strms**: 4

---

alpha-rto *alpha_rto_dur*

Sets the alpha retransmission timeout duration (in seconds) for SCTP association between HNB and HNB-GW as an integer from 0 through 65535. A "zero" value disables the timer in this configuration. Default: 5

---

beta-rto *beta_rto_dur*

Sets the beta retransmission timeout duration (in seconds) for SCTP association between HNB and HNB-GW an integer from 0 through 65535. A "zero" value disables the timer in this configuration. Default: 10

---

checksum-type [adler32 | crc32]

Sets the checksum algorithm type to be used in SCTP association between HNB and HNB-GW for packet validation. Default: CRC32
adler32: Specifies the SCTP association to use Adler32 checksum algorithm for packet validation. By default this is disabled.
crc32: Specifies the SCTP association to use 32-bit cyclic redundancy check (CRC) algorithm for packet validation. By default this is enabled.

---

cookie-life *cookie_life*

Sets the COOKIE life (in milliseocnds) for SCTP association between HNB and HNB-GW as an integer from 500 through 120000. Default: 600

---

max-retx [init | path | assoc] *max_retry*

Sets the maximum number of retries allowed in SCTP states for SCTP association between HNB and HNB-GW.
init: Sets the maximum attempts allowed after T1-init timer expires. If the T1-init timer expires then the HNB-GW retransmits INIT chunk and re-start the T1-init timer without changing state. This is repeated up to the configured times with this configuration. After that, the HNB-GW aborts the initialization process. Default number of attempts *max_retry* for this state is 5.
path: Sets the maximum attempts allowed after T3-rtx timer expires. Each time the T3-rtx timer expires on any address, or when a HEARTBEAT sent to an idle address is not acknowledged within a RTO, the error counter of that destination address incremented. When the value in the error counter exceeds this protocol parameter of that HNB address, the HNB-GW marks the destination transport address as inactive. Default number of attempts *max_retry* for this state is 5.

assoc: Sets the maximum number of consecutive retransmissions to its peer is allowed. If the value of this counter exceeds the limit configured with this keyword the HNB-GW considers the peer HNB unreachable and stop transmitting any more data to it. The SCTP association is automatically closed when the peer endpoint becomes unreachable. Default number of attempts *max_retry* for this state is 10.
max_retry is an integer from 1 through 255.

---

mtu-size [min | max | sart] *mtu_byte*

Sets the maximum transmission unit (MTU) size in Bytes for SCTP association between HNB and HNB-GW.
min: Sets the minimum size of MTU for SCTP association between HNB and HNB-GW. Default minimum MTU size *mtu_byte* is 508 Bytes.
max: Sets the maximum size of MTU for SCTP association between HNB and HNB-GW. Default maximum MTU size *mtu_byte* is 1500 Bytes.
start: Sets the size of MTU for SCTP association at the start of session between HNB and HNB-GW. Default MTU size *mtu_byte* at initial sate is 508 Bytes.
mtu_byte is an integer from 508 to 65535.

---

rto { initial *ini_rto_dur* **| min** *min_rto_dur* **| max** *max_rto_dur* **}**

Sets the Retransmission TimeOut (RTO) duration parameters for SCTP association between HNB and HNB-GW.
initial *ini_rto_dur*: Sets the initial retransmission timeout duration (in seocnds) for SCTP association between HNB and HNB-GW as an integer from 1 through 1200. Default: 30.
min *min_rto_dur*: Sets the minimal retransmission timeout duration (in seconds) for SCTP association between HNB and HNB-GW as an integer from 1 through 50. Default: 10
max *max_rto_dur*: Sets the maximum retransmission timeout duration (in secinds) for SCTP association between HNB and HNB-GW as an integer from 5 through 1200. Default: 600.

---

sack-frequency *sack_frq*

Sets the number of chunks received before sending the Selective Acknowledgement chunk HNB from HNB-GW in SCTP association. the SACK chunk is sent to the HNB to acknowledge received DATA chunks and to inform the HNB of gaps in subsequently received DATA chunks.
sack_frq is the frequency after which SACK chunk is sent to HNB specified as an integer from 1 through 5. Default: 2

---

sack-period *sack_dur*

Sets the duration (in seconds) after which Selective Acknowledgement chunk is sent to HNB from HNB-GW in SCTP association. The SACK chunk is sent to the HNB to acknowledge received DATA chunks and to inform the HNB of gaps in subsequently received DATA chunks.
sack_dur is an integer from 0 through 5. A “zero” value disables the parameter.

---

max-in-strms *in_strms*

Sets the maximum number of inward SCTP streams allowed on HNB-GW for an associated HNB in an SCTP association as an integer from 1 through 16. Default: 4

---

max-out-strms *out_strms*

Sets the maximum number of outgoing SCTP streams allowed from HNB-GW for an associated HNB in an SCTP association as an integer from 1 through 16. Default: 4

Usage

Use this command to configure the SCTP protocol messaging and session management parameters in SCTP association between HNB and HNB-GW.

Example

The following command sets the SCTP COOKIE life to *600* milliseconds on HNB-GW for the SCTP association:

```
default sctp cookie-life
```

sctp bind

Configures the SCTP IP address and port that is used for binding the SCTP socket to communicate with the Home-NodeB over an Iuh interface within an HNB-GW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

sctp bind { address *address* **| port** *port_num* **}**

[default | no] sctp bind { address | port }

default

Sets the SCTP port to the default value of 600.

address *address*

Specifies the IP address of the HNB-GW Iuh interface in IPv4 dotted-decimal or IPv6 colon-separated notation.

port *port_num*

Specifies the SCTP port number to communicate with the Home-NodeBs using Iuh interface as an integer form 1 through 65535.

Usage

Use this command to assign the SCTP IP address and port with SCTP socket on HNB-GW to communicate with the Home-NodeB using Iuh interface. This SCTP configuration provides the IP-address and listen port where HNB-GW service shall bind to listen for incoming SCTP associations from HNB.

Example

The following command sets the SCTP port number *999* on HNB-GW to listen from Home-NodeB over Iuh interface:

```
sctp bind port 999
```

The following command sets the SCTP address *10.2.3.4* of HNB-GW to use with Home-NodeB over Iuh interface:

```
sctp bind address 10.2.3.4
```

sctp connection-timeout

Configures the SCTP connection timeout duration to explicitly remove the SCTP association with a non-responsive HNB in an HNB-GW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

sctp connection-timeout *dur*

[default | no] sctp connection-timeout

no

Disables the connection time out configuration on HNB-GW service.

default

Restores the connection timeout duration value to its default value of 10 seconds.

dur

Sets the connection timeout duration (in seconds) after which the association is explicitly removed. In case of an HNB de-registration scenario, the HNB-GW waits for configured amount time before initiating the procedure to clear the SCTP association.
dur is an integer from 5 through 30. Default: 10

Usage

Use this command to configure the minimum duration value before removing the SCTP association between a non-responding HNB and HNB-GW. If HNB registration not happened within the configured period after the SCTP association is established then the SCTP association is explicitly removed. In a scenario where an HNB de-registered due to any reason, the HNB-GW waits for the configured amount of time before initiating the procedure to clear the SCTP association.

Example

The following command sets the SCTP connection timeout duration to *15* second on HNB-GW after expiry of which the SCTP association is removed:

```
sctp connection-timeout 15
```

sctp heart-beat-timeout

Configures the SCTP heartbeat timer parameters for SCTP connection over an IuH interface in an HNB-GW service instance.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

sctp heart-beat-timeout *dur*

[default | no] sctp heart-beat-timeout

no

Disables the heartbeat timer configuration for SCTP over IuH in HNB-GW service instance.

default

Restores the default time out value for heartbeat timer to 30 seconds.

dur

Sets the heartbeat timer timeout duration (in seconds) after which the next heartbeat command is sent to HNB from HNB-GW in SCTP over an IuH interface. In an HNB de-registration scenario, the HNB-GW waits for configured amount time before initiating the procedure to clear the SCTP association.
dur is an integer from 1 through 300. Default: 30

Usage

Use this command to configure the minimum duration value before retransmitting the HEARTBEAT chunk to HNB from HNB-GW in SCTP transmission. By default HNB-GW monitors the reachability of the idle HNBs by sending a HEARTBEAT chunk periodically to the HNB address.
Each time the HEARTBEAT timer expires on any address, or when a HEARTBEAT sent to an idle address is not acknowledged within a Retransmission Timeout duration, the error counter of that HNB incremented. When the value in the error counter exceeds the protocol parameter for maximum retransmission for that destination address, the HNB-GW mark the destination HNB as inactive and a notification is sent to the upper layer.

Example

The following command sets the SCTP HEARTBEAT timeout duration to *15* second on HNB-GW after expiry of which the HNB-GW retransmits the HEARTBAT chunk to HNB over SCTP association:

```
sctp heart-beat-timeout 15
```

security-gateway aaa

Associates a pre-configured AAA Service group to use authentication parameters for Security Gateway (SeGW) functionality in HNB-GW service. The associated AAA server group is a pre-configured via Context Configuration mode.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

security-gateway aaa authentication { first-phase | second-phase } context *ctx_name* **aaa-group** *aaa_grp*

no security-gateway aaa { attribute calling-station-id | authentication { first-phase | second-phase }

no

Removes previously configured AAA authentication or attribute setting from HNB-GW service while using SeGW functionary.

attribute calling-station-id *ms_id*

Specifies the calling station identifier from where the user placed the call.

authentication { first-phase | second-phase } context *ctx_name* **aaa-group** *aaa_grp*

Specifies the AAA authentication parameters to be used while using SeGW functionality in an HNB-GW service.
first-phase: Specifies the parameters to be used for first phase of authentication while using SeGW functionality in an HNB-GW service. This associates the AAA parameters through AAA server group association with in it.
second-phase: Specifies the parameters to be used for second phase of authentication while using SeGW functionality in an HNB-GW service. This associates the AAA parameters through AAA server group association with in it.
context *ctx_name*: Specifies the name of the context to be used for first/second or both phases of authentication.
aaa-group *aaa_grp*: Specifies the name of the AAA server group configured via Context Configuration mode with AAA parameters that will be used for first/second or both phases of authentication.

Important: For more information on AAA server groups, refer *AAA Server Group Configuration Mode Commands*.

Usage

Use this command to associate or tie the AAA authentication or attribute parameters with an HNB-GW service which is to be used for first/second or both phase of authentication while using SeGW functionality in

an HNB-GW service or removing AAA attribute “calling-station-id” from AAA message. This functionality is part of SeGW configuration support in an HNB-GW service.

Caution: This is a critical configuration and need to be configured carefully when Security Gateway (SeGW) functionality required on HNB-GW service.

Example

The following command associates an AAA server group named *sec_gw_grp1* with HNB-GW service to use specific AAA authentication parameters in first phase of authentication and another AAA server group named *sec_gw_grp2* to use different AAA authentication parameter in second phase of authentication. Both AAA server groups are configured in same context named *SeGW_ctx1*:

```
security-gateway aaa authentication first-phase context SeGW1 aaa-group
sec_gw_grp1security-gateway aaa authentication second-phase context SeGW1
aaa-group sec_gw_grp2
```

The following command disables a previously configured AAA authentication parameter for first phase of authentication:

```
no security-gateway aaa authentication first-phase
```

security-gateway bind

Binds the SeGW in an HNB-GW service to a logical IP interface serving as an Iuh interface and associates an IPsec IKEv2 crypto-map template.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

security-gateway bind address *address* **crypto-template** *cryp_name* **[context** *ctxt_name***]**

no security-gateway bind

no

Removes a previously configured IPSec IP address use for binding the IKEv2 IPSec tunnel (local bind address) to communicate with the Home-NodeBs using Iuh interface.

bind address *address*

Specifies the IP address for the Iuh interface for the IPSec tunnel. This is the IP address where the HNB-GW service is bound and that is provided to the Home-NodeB during HNB-GW discovery.
The IP address is expressed in IPv4 dotted-decimal or IPv6 colon-separated notation.

crypto-template *cryp_name*

Specifies the Crypto-map template to be used for IPsec IKEv2 tunneling for the interface configured as an Iuh.
cryp_name specifies the name of the pre-configured Crypto-map template which is configured in Crypto-Map Template Configuration mode and associated with the HNB-GW service to create an IPSec tunnel with a Home-NodeB during HNB-GW discovery procedure over an Iuh interface.

context *ctx_name*

Specifies the name of the pre-configured context in which the Security Gateway service is configured. By default this command uses the HNB-GW service context for the ecurity Gateway configuration.

Usage

Use this command to associate or tie the HNB-GW service to a specific logical IP address that is used for binding the Iuh socket to communicate with the Home-NodeB using IPSec tunnel. A maximum of one IP address can be configured with this command for one HNB-GW service.
The HNB-GW passes the IP address during setting up the HNB-GW discovery procedure with the Home-NodeB.

Caution: This is a critical configuration. The HNB-GW service cannot be started without this configuration. Any change to this configuration would lead to restarting the HNB-GW service and removing or disabling this configuration stops the HNB-GW service.

Example

The following command binds the logical IP interface with the address of *10.2.3.4* to the HNB-GW service using existing IPsec Crypto-Map template *crypto1* to establish IPSec tunnel with Home-NodeB:

```
security-gateway bind address 10.2.3.4 crypto-template crypto1
```

The following command disables a binding that was previously configured:

```
security-gateway bind address
```

security-gateway username

Configures the options related to user name received from MS.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no | defualt ] security-gateway username mac-address-stripping
```

no

Disables previously configured option for user name received from MS.

default

Sets the user name option configuration of default setting of "Disable".

mac-address-stripping

Sets the system to strip the MAC address from the user name received from the MS. Default: Disabled

Usage

Use this command to set the user name related options. By enabling this option system trips the MAC address from the user name received from MS.

Example

The following command sets the system to strip the MAC address from user name received from user MS:

```
security-gateway username mac-address-stripping
```

tnnsf-timer

Configures the NAS Node Selection Function (NNSF) timer (T-NNSF) which is used by the HNB-GW to store the IMSI and the relevant Global-CN-ID in the short term after Paging. This timer is used for Iu-Flex feature support.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

tnnsf-timer *dur*

[no | default] tnnsf-timer

no

Disables/removes the configured timer value of NNSF timer (T-NNSF) from HNB-GW service instance.

default

Sets the timer value of NNSF timer (T-NNSF) for HNB-GW service instance to default value of 30 seconds.

tnnsf-timer *dur*

Configures the NNSF timer (in seconds) which is used by the HNB-GW to store the IMSI and the relevant Global-CN-ID as an integer from 10 through 60. Default: 30

Usage

Use this command to configure the NNSF timer value in seconds for Iu-Flex support.
Whenever the MSC sends the paging request with IMSI, the HNB-GW stores the Global_CN_ID of the node which issued the paging request message for the given IMSI and HNB-GW starts the **tnnsf-timer**. HNBGW stores the mapping of IMSI to Global_CN_ID until the **tnnsf-timer** expires

Example

The following command sets the NNSF timer value to *30* seconds in an HNB-GW service instance:

```
default tnssf-timer
```

ue registration-timeout

Configures the UE registration timeout duration to de-register the connected UE from an HNB-GW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

```
ue registration-timeout dur

[ default | no ] ue registration-timeout
```

no

Disables the UE registration timeout duration and explicitly de-registers UE from the HNB-GW service.

default

Restores the UE registration timeout duration value to its default value of 120 seconds.

dur

Sets the UE registration timeout duration (in seconds) after which the UE is de-registered from HNB-GW. In a scenario when all Iu connections are released for a subscriber, the HNB-GW service de-registers the UE after cthe onfigured duration only.
dur is an integer from 60 through 300. Default: 120

Usage

Use this command to configure the minimum duration value before de-registering the UE when subscriber fails to establish the Iu connection. If subscriber's Iu session does not established before configured period then UE is de-registered. Also in a scenario where all Iu connections are released for a subscriber, the HNB-GW service waits for configured period before starting UE deregistration procedure.

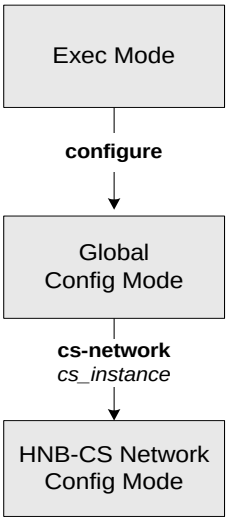
Example

The following command sets the UE registration timeout duration to *150* second on HNB-GW after expiry of which the UE is de-registered:

```
ue registration-timeout 150
```

Chapter 145
HNB-CS Network Configuration Mode Commands

The HNB-CS Network configuration mode provides the commands to create, provide, and manage the circuit switched (CS) network instance allowing the Home Evolved NodeB Gateway (HNB-GW) access with the CS core network in a 3G UMTS network.



associate alcap-service

Associates a previously defined Access Link Control Application Part (ALCAP) service with the CS network instance for multiplexing of different users onto one AAL2 transmission path using channel IDs (CIDs). This configuration is provided to support IuCS-over-ATM functionality

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

associate alcap-service *svc_name* **context** *ctx_name*

no associate alcap-service

no

Removes the associated ALCAP service from this HNB-CS network instance configuration.

svc_name

Identifies the name of the ALCAP service preconfigured in Context configuration mode to associate with an HNB-CS network instance for multiplexing of different users onto one AAL2 transmission path using channel IDs (CIDs).
svc_name must be a preconfigured ALCAP service.
Only one instance of this command can be configured.

Caution: If this CLI is not configured any RAB-ASST-REQ requesting AAL2 connection setup shall be rejected with an appropriate cause.

context*ctx_name*

Specifies the name of the context in which ALCAP service is configured.
ctx_name must be an existing context name in which this ALCAP service is configured.

Usage

Use this command to configure IuCS-over-ATM support. This association of ALCAP protocol service configuration in HNB-CS network instance provides multiplexing of different users onto one AAL2 transmission path using channel IDs (CIDs).

Caution: If this CLI is not configured any RAB-ASST-REQ message requesting AAL2 connection setup shall be rejected with an appropriate cause.

Important: This command must not be used more than once to configure IuCS-over-ATM support.

Example

Following command associates ALCAP service *alcap_svc1* configured in context named *Ctx_alcap1* with specific HNB-CS network instance:

```
associate alcap-service alcap_svc1context ctx_alcap1
```

associate rtp pool

Associates a previously defined RTP pool (IP pool) with the CS network instance to be used for assignment of IP address/port as RTP streams end point address over IuCS interface. This configuration support is provided for RTP stream management feature in an HNB-GW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

associate rtp pool *pool_name* **context** *ctx_name*

no associate rtp pool

no

Removes the associated RTP pool (IP pool) from this HNB-CS network instance configuration.

pool_name

Identifies the name of the RTP IP pool preconfigured in Context configuration mode to associate with an HNB-CS network instance to be used for assignment of IP address/port over the IuCS interface RTP streams. *pool_name* must be an existing IP pool name configured in Context configuration mode.

Important: For IP pool (RTP pool) configuration, refer *Context Configuration Commands Mode* chapter.

context*ctx_name*

Specifies the name of the context in which RTP pool (IP pool) is configured.
ctx_name must be an existing context name in which this IP pool is configured.

Usage

Use this command to associate RTP pool (IP Pool) with an HNB-CS network instance for allotment of IP address/port over IuCS interface for RTP streams across all sessions. A fixed range of RTP ports from 5000 through 65000 shall be used to allocate to RTP stream.

Important: This command must be used to provide IP address/port for RTP streams end point address over IuCS interface.

Important: This configuration support is provided for RTP stream management feature on an HNB-GW service.

Example

Following command associates RTP pool named *rtp_1* with specific HNB-CS network instance:

```
associate rtp pool rtp_1
```

associate sccp-network

Associates a predefined Signaling Connection Control Part (SCCP) network id with the CS network instance in order to route the messages towards MSC/VLR over IuCS interface.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

associate-sccp-network *sccp_net_id*

no associate-sccp-network

no

Removes the associated SCCP network id from this HNB-CS network instance configuration.

sccp_network_id

Identifies the predefined SCCP network id to associate with an HNB-CS network instance over IuCS/IuFlex interface to enable connection with MSC/VLR(s).
sccp_network_id must be a predefined SCCP network id in Global configuration mode.

Usage

Use this command to associate a preconfigured SCCP network id over IuCS interface in HNB-GW service to connect with CS network elements; i.e. MSC.

Caution: The SCCP network id must be defined in Global Configuration mode before using it with this command.

Important: A single SCCP network configuration instance can not be shared with multiple HNB-CS network instances.

Example

Following command associates SCCP network *2* with specific HNB-CS network instance:

```
associate-sccp-network 2
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

map core-network-id

Maps/associates the CS core network id to a default Mobile Switching Center (MSC) in network using MSC point code in HNB-CS network to allow HNBs to access UMTS network.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

map core-network-id *cn_id* **point-code** *msc_point_code*

no map core-network-id *cn_id*

no

Removes the mapping of a CS core network id with particular MSC point code.

cn_id

Specifies the core network identifier configured to represent a UMTS CS core network as an integer from 0 through 4095.
Multiple instance of this command can be mapped with different MSC point code.

point-code *msc_point_code*

Specifies the SS7 address of the default MSC in the CS network in point code value to a configured HNB-CS network instance.
point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.
Only one instance of this MSC point code can be mapped with one CS core network id.

Usage

Use this command to map a UMTS CS core network identifier with a particular MSC point code.
This command can be entered multiple times with same MSC point code to map with one or more CS core network Id, but a particular core network identifier can be mapped to one MSC only.
This command is instrumental in Iu-Flex functionality, whenever HNB-GW receives RESET/RESET-RES messages from MSC with Global CN-ID information element, the response from HNB-GW is sent to the node configured for that particular Global CN-ID.
If the RESET/RESET-RES messages do not have Global CN-ID IE, then the response of those messages is directed to the default MSC which is configured using **msc point-code** command in this mode.

Example

The following command configures the CS core network identifier *101* with an MSC point code *1.2.3*:

```
map core-network-id 101 point-code 1.2.3
```

The following command configures the CS core network identifier *102* with the same MSC point code *1.2.3*:

```
map core-network-id 102 point-code 1.2.3
```

map idnns

Configures the mapping of Intra-Domain NAS Node Selector (IDNNS) IE received from UE in RUA connect message towards HNB-GW to MSC point code. This is an important configuration for CS network resource sharing over Iu-Flex interface.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

map idnns range *idnns_start* **to** *idnns_end* **point-code** *msc_point_code* **[backup point-code** *bkup_msc_point_code***]**

no map idnns range *idnns_start* **to** *idnss_end*

no

Removes the entries of mapping of range of IDNNS received from UE with particular MSC point code.

range *idnns_start* **to** *idnns_end*

Specifies the range of IDNNS received from the UE to map with a particular MSC point code during initial CS core network node selection.
idnns_start is an integer from 0 through 1023 that should be less than *idnns_end*.
idnns_end must be an integer from 0 through 1023 that should be more than *idnns_start*.
The command can be entered more than once to map multiple IDNNS ranges to the same MSC, but overlapping and mapping of the same range to different MSC point codes is not allowed.

point-code *msc_point_code*

Specifies the SS7 address of the MSC in the CS network to map with a range of IDNNS values.
msc_point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.

backup point-code *bkup_msc_point_code*

Specifies the SS7 address of the MSC to be used as a backup in the CS network to map with a range of IDNNS values.
bkup_msc_point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.

Usage

Use this command to map a NRI received from UE during initial CS network node selection to MSC point code through NRI range mapping over Iu-Flex interface.
The IDNNS refers to the information element in RUA connect message from UE towards RAN (HNB-GW). In IDNNS IE, if the choice of routing mentioned is other than local P-TMSI, then the value it provides is used against this configuration to map the MSC point code.
If backup MSC point-code is specified, then specified MSC works as backup for the IDNS range configured. This Backup MSC is selected if the mapped MSC for a given IDNNS range is going for offloading using **offload-msc point-code** command.

The command can be entered more than once to map multiple IDNNS ranges to same MSC point code, but overlapping and mapping of same range to different MSC point code is not allowed.

Example

The following command maps the IDNNS range from *101* to *201* with MSC point code *1.2.3* and point code *7.8.9* as backup MSC point code:

```
map nri range 101 to 201 point-code 1.2.3 backup point-code 7.8.9
```

The following command removes all IDNNS range matching entries between *301* to *399* from the configuration:

```
no map idnns range 301 to 399
```

map lac

Configures the mapping of the Location Area Code (LAC) received from UE to an MSC point code. This is an important configuration for CS network resource sharing without Iu-Flex interface configuration.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

map lac range *lac_start* **to** *lac_end* **point-code** *msc_point_code*

no map lac range *lac_start* **to** *lac_end*

no

Removes the entries of mapping of range of LACs received from UE with particular MSC point code.

range *lac_start* **to** *lac_end*

Specifies the range of LACs received from UE to map with particular MSC point code during initial CS core network node selection.
lac_start is an integer from 0 through 65535 that should be less than *lac_end*.
lac_end is an integer from 0 through 65535 that should be more than *lac_start*.
The command can be entered more than once to map multiple LAC ranges to same MSC, but overlapping is not allowed.

point-code *msc_point_code*

Specifies the SS7 address of the MSC in the CS network to map with a range of LAC values.
point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.

Usage

Use this command to map a LAC, received from UE during HNB registration, for MSC selection over IuCS interface through LAC range mapping with MSC point code.
This configuration is used during initial CS core network node selection when the LAC from the UE is available. This configuration is used when the core network is not using Iu-Flex interface for MSC selection.
The command can be entered more than once to map multiple LAC ranges to same MSC point code.

Important: This command can be used together with Iu-Flex configuration, but MSC selection based on LAC takes place only if Iu-Flex is not configured. If both Iu-Flex and LAC are configured then selection of MSC is based on Iu-Flex configuration only.

Example

The following command maps the LAC range from *20* to *50* with MSC point code *1.2.3*:

```
map lac range 20 to 50 point-code 1.2.3
```

The following command removes all LAC range matching entries between *20* to *50* from the configuration:

```
no map lac range 20 to 50
```

map nri

Configures the mapping of Network Resource Identifier (NRI) sent from UE to the MSC point code. This is an important configuration for CS network resource sharing over Iu-Flex interface.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

map nri range *nri_start* **to** *nri_end* **point-code** *msc_point_code*

no map nri range *nri_start* **to** *nri_end*

no

Removes the entries of mapping of range of NRIs received from UE with particular MSC point code.

range *nri_start* **to** *nri_end*

Specifies the range of NRIs received from UE to map with pa articular MSC point code during initial CS core network node selection.
nri_start is an integer from 0 through 1023 that should be less than *nri_end*.
nri_end is an integer from 0 through 1023 that should be more than *nri_start*.
The command can be entered more than once to map multiple NRI ranges to same MSC, but overlapping is not allowed.

point-code *msc_point_code*

Specifies the SS7 address of the MSC in the CS network to map with a range of NRI values.
point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.

Usage

Use this command to map a NRI received from UE during initial CS network node selection to MSC point code through NRI range mapping over Iu-Flex interface.
This configuration is used during initial CS core network node selection when the network resource identifier (NRI) from the UE is available. The NRI range is mapped to MSC point code. This configuration is used when the core network uses Iu-Flex interface.
The command can be entered more than once to map multiple NRI ranges to same MSC point code.
It is possible to configure multiple ranges to more than one MSC however this configuration is required only when the CS core network is configured as Multi-Operator Core Network (MOCN).
When the CS core network is not MOCN and one range is mapped to more than one MSC then MSC is selected randomly in a non-predictable manner.

Example

The following command maps the NRI range from *101* to *201* with MSC point code *1.2.3*:

```
map nri range 101 to 201 point-code 1.2.3
```

The following command maps the NRI range from *301* to *399* with MSC point code *1.2.3*:

```
map nri range 301 to 399 point-code 1.2.3
```

The following command removes all NRI range matching entries between *301* to *399* from the configuration:

```
no map nri range 301 to 399
```

msc deadtime

Configures a timer on the HNB-GW to manage MSC availability in a CS core network on receiving of a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from an SCCP instance.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

msc deadtime { immidiate |*dur* }

[no | default] msc deaddtime

no

Marks the peer node (MSC) as always available; it can never be marked down for a specific HNB-CS network instance.

default

Sets the default action for HNB-GW and provisions it as such that the peer node (MSC) is marked down as soon as HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP in a specific HNB-CS network instance. Default: Enabled

immidiate

Sets the HNB-GW to mark the peer node (MSC) down immediately and clears all Iu-CS connections towards the MSC. Default: Disabled

dur

Sets the duration (in seconds) for a timer that starts when the HNB-GW receives a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer MSC. On expiry of this timer the peer MSC is marked as dead and all Iu-CS connections towards that MSC are released.
dur is an integer from 1 through 30.
Only one instance of this command can be configured.

Usage

This command is used to configure a timer on HNB-GW to manage MSC availability in a CS core network on receiving of PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP. This configuration plays important role during RANAP reset procedure as well.
Timer value sets the duration in seconds for a timer which started once HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer MSC. On expiry of this timer the peer MSC is marked as dead and all Iu-CS connections towards that MSC shall be released.

Important: This command can be entered only once. Reentering this command overwrites the previous parameters.

Example

The following command configures the deadtime timer value for *10* seconds on HNB-GW. Once HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer MSC the HNB-GW waits for configured period and on expiry of timer it marks the specific MSC as dead:

```
msc deadtime 10
```

msc point-code

Configures the default MSC point-code within an HNB-CS network instance. This command is used when HNB-GW is to be connected to only one MSC with in a CS network or as default MSC for all HNBs connected through specific HNB-CS network instance.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

`[ no ] msc point-code` *`point_code`*

`no`

Removes the configured default MSC point code from a specific HNB-CS network instance.

Caution: Removing the MSC point code is a disruptive operation and affects all HNB sessions which are connected to particular MSC through an HNB-CS network instance.

`msc` *`point_code`*

Specifies the SS7 address of the default MSC in the CS network to this configured HNB-CS network instance.
`point_code` is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.
Only one instance of this command can be configured.

Usage

Use this command to configure a default MSC to which HNB connects for CS network access through HNB-GW service.
Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC Range.
- a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

Important: This command can be entered only once. If entered again the previous value shall be overwritten.

Example

The following command configures a default MSC with point code *`101.201.101`* for HNBs to access CS network through HNB-GW service in this HNB-CS network instance:

```
msc point-code 101.201.101
```

nri length

Configures the network resource identifier (NRI) length in bits to identify a specific MSC serving in a pooled area. At least one NRI value has to be assigned to an MSC serving in a pool. The NRI is coded inside of the temporary mobile subscriber identity (TMSI), located within bits 14 to 23 with an variable length between 0 and 10 bits. Operator needs to set this NRI length to indicates the number of bits that shall be used for the NRI field to set the parameters for Iu-Flex (MSC pooling) functionality.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

nri length *nri_value*

default nri length

default

Sets the NRI length to the default value of 0 and disables the Iu-Flex (MSC pooling) functionality.

nri length *nri_value*

Default: 0
Specifies the number of bits to be used in the P-TMSI (bits 23 to 18) to define the network resource identifier (NRI). The NRI length configuration also sets the maximum size of the pool. If not configured, the NRI length is of zero length.
length is an integer from 1 to 10 that identifies the number of bits. When a non-zero value is configured the CS network is considered to be a pool.

Usage

Use this command to enable the Iu-Flex functionality on HNB-GW. This command identifies a unique MSC serving a pooled area for Iu-Flex functionality and at least one NRI value has to assigned to an MSC serving in a pool. It performs MSC pooling/offloading scenario over Iu-Flex interface. The NRI is stored in the bits 14 to 23 of TMSI. The HNB-GW uses a portion of this NRI to set the parameters for Iu-Flex (MSC pooling) functionality.
If more than one NRI is configured, the HNB-GW service does round-robin between the available NRIs when new subscriber(s) (re)connect.
This command must be used in conjunction with **null nri** command to configured MSC pooling/offloading over Iu-Flex interface.

Example

The following command sets the HNB-GW to a bit length of *6* to derive the values from the NRI field (stored in bits 14 to 23 of TMSI) to set the parameters for Iu-Flex (MSC pooling) functionality:

```
nri length 6
```

null-nri

Configures the null NRI for load redistribution in support of Iu-Flex functionality. The NRI value defined with this command must be unique across the pool areas. This null-NRI is used by HNB-GW for load redistribution during MSC offloading.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

null-nri *null_nri_value*

no null-nri *null_nri_value*

no

Disables/removes the configured null-NRI value used for MSC offloading procedure.

null_nri_value

Specifies the null-NRI value to be used by HNB-GW for load re-distribution during MSC offloading as an integer from 0 through 1023.
Without MOCN configuration this value can be entered only once.
For MOCN a unique null-NRI must be assigned to each MOCN operator identified by its PLMN-ID (MCC+MNC).
A 0 (zero) value configured as a null-NRI indicates the keyword is not to be used. There is no default value for this parameter.

Usage

Use this command to identify the MSC to be used by HNB-GW for load redistribution during MSC offloading over an Iu-Flex interface.
There is one unique null-NRI in a PLMN supporting pool functionality.
Without MOCN configuration this command can be entered only once. For MOCN a unique null-NRI must be assigned to each MOCN operator identified by its PLMN-ID (MCC+MNC).

Example

The following command sets the null-NRI as *1001* to be used by HNB-GW for load redistribution during MSC offloading:

```
null-nri 1001
```

offload-msc

Provisions the HNB-GW to enable or disable the exclusion of a particular primary MSC node during an NAS Node Selection Function (NNSF) procedure when it needs to be offloaded while using Iu-Flex functionality on the HNB-GW.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

[no] offload-msc point-code *msc_point_code*

no

Removes the specified primary MSC point code from the exclusion list for NNSF function on HNB-GW and re-enables the inclusion of the primary MSC to be considered by HNB-GW.

point-code *msc_point_code*

Specifies the SS7 address of the primary MSC in the CS network to be excluded for NNSF function on HNB-GW when it needs to be offloaded via Iu-Flex functionality.
point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.
Only one instance of this primary MSC point code can be mapped with one CS core network id.

Usage

Use this command to provision the HNB-GW to enable or disable the exclusion of the primary MSC node when it needs to be offloaded.
When this command is enabled for exclusion of primary MSC node during NNSF function in HNB-GW, the HNB-GW excludes the particular node from being considered.
User can re-enable the inclusion of the primary MSC node to be considered for NNSF functionality by **no offload-msc point-code** command.

Important: Offload check is only for the primary point code and NOT for the backup point code.

This command can be used for planned maintenance as well.

Example

The following command configures the HNB-GW to exclude the primary MSC point code *1.2.3* from being considered in NSSF function for Iu-Flex support:

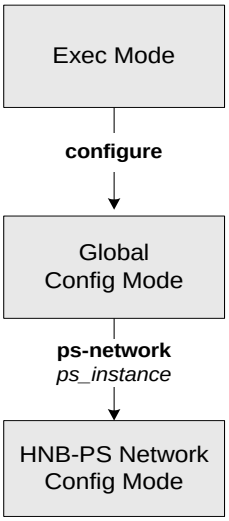
```
offload-msc point-code 1.2.3
```

The following command re-enables the inclusion of MSC point code *1.2.3* from being considered in NSSF function for Iu-Flex support:

```
no offload-msc point-code 1.2.3
```

Chapter 146
HNB-PS Network Configuration Mode Commands

The HNB-PS Network Configuration Mode is used to manage the packet switched (PS) network instance on HNB-GW service to provide HNB access with the PS core network in a 3G UMTS network.



associate gtpu-service

Associates a previously configured GTP-U service to provide a GTP-U tunnel with an SGSN towards the core network side. A GTP-U service must be configured in Context Configuration mode before using this configuration.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

associate gtpu-service *svc_name* **context** *ctx_name*

no associate gtpu-service

no

Removes the associated GTP-U service from this HNB-GW service configuration.

svc_name

Specifies the name of the preconfigured GTP-U service.

context *ctx_name*

Specifies the name of the context in which the GTP-U service is configured.

Usage

Use this command to configure GTP-U data plan tunnel between HNB-GW service and GSNs in core network. The service defined for GTP-U tunnel must be configured in Context configuration mode.

Important: Another GTP-U service can be used to bind the HNB-GW service to GTP-U tunnel with HNB in HNB access network and can be configured in HNB-GW Service Configuration mode. For more information on GTP-U service configuration, refer to *GTP-U Service Configuration Mode Commands* chapter.

Example

The following command associates GTP-U service *gtpu_svc1* configured in context named *Ctx_gtpu1* with specific HNB-PS network instance for GTP-U tunnel towards GSN in core network:

```
associate gtpu-service gtpu_svc1 context Ctx_gtpu1
```

associate-sccp-network

Associates a previously defined Signaling Connection Control Part (SCCP) network identifier with the PS network instance in order to route the messages towards the SGSN via the IuPS interface.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

associate-sccp-network *sccp_net_id*

no associate-sccp-network

no

Removes the associated SCCP network configuration instance from this HNB-PS network instance configuration.

sccp_net_id

Specifies a predefined SCCP network identifier.

Usage

Use this command to associate a predefined SCCP network id with the IuPS interface in HNB-GW service to connect with PS network elements; i.e. SGSN.

Caution: The SCCP network id must be defined in Global Configuration mode before using it with this command.

Important: A single SCCP network id can not be shared with multiple HNB-PS network instances.

Example

The following command associates SCCP network id *2* with specific HNB-PS network instance:

```
associate-sccp-network 2
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

map core-network-id

Maps/associates the PS core network identifier to a default SGSN in the network using an SGSN point code to allow HNBs to access the UMTS network.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

map core-network-id *cn_id* **point-code** *sgsn_point_code*

no map core-network-id *cn_id*

no

Removes the mapping of a PS core network id with particular SGSN point code.

cn_id

Specifies the core network identifier configured to represent a UMTS PS core network as n integer from 0 through 4095.
Multiple instance of this command can be mapped with different SGSN point codes.

point-code *sgsn_point_code*

Specifies the SS7 address of the default SGSN in the PS network.
point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.
Only one instance of this SGSN point code can be mapped with one PS core network identifier.

Usage

Use this command to map a UMTS PS core network identifier with a particular SGSN point code.
This command can be entered multiple times with same SGSN point code to map with one or more PS core network Id, but a particular core network identifier can be mapped to one SGSN only.
This command is instrumental in Iu-Flex functionality, whenever HNB-GW receives RESET/RESET-RES messages from SGSN with Global CN-ID information element, the response from HNB-GW is sent to the node configured for that particular Global CN-ID.
If the RESET/RESET-RES messages do not have Global CN-ID IE, then the response of those messages is directed to the default SGSN which is configured using **sgsn point-code** command in this mode.

Example

The following command configures the PS core network identifier *101* with an SGSN point code *1.2.3*:

```
map core-network-id 101 point-code 1.2.3
```

The following command configures the PS core network identifier *102* with the same SGSN point code *1.2.3*:

```
map core-network-id 102 point-code 1.2.3
```

map idnns range

Configures the mapping of an Intra-Domain NAS Node Selector (IDNNS) IE received from UE in an RUA connect message towards HNB-GW. This is an important configuration for PS network resource sharing over an Iu-Flex interface.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

map idnns range *idnns_start* **to** *idnns_end* **point-code** *sgsn_point_code* [**backup point-code** *bkup_sgsn_point_code*]

no map idnns range *idnns_start* **to** *idnns_end*

no

Removes the entries of mapping of range of IDNNS received from UE with particular SGSN point code.

range *idnns_start* **to** *idnns_end*

Specifies the range of IDNNSs received from UE to map with particular SGSN point codes during the initial PS core network node selection.
idnns_start is an integer from 0 through 1023 that should be less than *idnns_end*.
idnns_end is an integer from 0 through 1023 that should be more than *idnns_start*.
The command can be entered more than once to map multiple IDNNS ranges to the same SGSN. However, overlapping and mapping of the same range to different SGSN point codes is not allowed.

point-code *sgsn_point_code*

Specifies the SS7 address of the SGSN in the PS network.
sgsn_point_code is ann SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.

backup point-code *bkup_sgsn_point_code*

Specifies the SS7 address of the SGSN to be used as the backup in the PS network.
bkup_sgsn_point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.

Usage

Use this command to map a NRI received from UE during initial PS network node selection to SGSN point code through NRI range mapping over Iu-Flex interface.
The IDNNS refers to the information element in RUA connect message from UE towards RAN (HNB-GW). In IDNNS IE, if the choice of routing mentioned is other than local P-TMSI, then the value it provides is used against this configuration to map the SGSN point code.
If backup SGSN point-code is specified, then specified SGSN works as backup for the IDNS range configured. This Backup SGSN is selected if the mapped SGSN for a given IDNNS range is going for offloading using **offload-sgsn point-code** command.

The command can be entered more than once to map multiple IDNNS ranges to same SGSN point code, but overlapping and mapping of same range to different SGSN point code is not allowed.

Example

The following command maps the IDNNS range from *101* to *201* with SGSN point code *1.2.3* and point code 7.8.9 as backup SGSN point code:

```
map nri range 101 to 201 point-code 1.2.3 backup point-code 7.8.9
```

The following command removes all IDNNS range matching entries between *301* to *399* from the configuration:

```
no map idnns range 301 to 399
```

map nri range

Configures the mapping of the Network Resource Identifier (NRI) received from UE to an SGSN point code. This is an important configuration for PS network resource sharing over Iu-Flex interface.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

map nri range *nri_start* **to** *nri_end* **point-code** *sgsn_point_code*

no map nri range *nri_start* **to** *nri_end*

no

Removes the entries of mapping of range of NRIs received from UE with a particular SGSN point code.

range *nri_start* **to** *nri_end*

Specifies the range of NRIs received from UE to map with a particular SGSN point code during initial PS core network node selection.
nri_start is an integer from 0 through 1023 that should be less than *nri_end*.
nri_end is an integer from 0 through 1023 that should be more than *nri_start*.
The command can be entered more than once to map multiple NRI ranges to the same SGSN, but overlapping is not allowed.

point-code *sgsn_point_code*

Specifies the SS7 address of the SGSN in the PS network to map with range of NRI values.
point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.

Usage

Use this command to map a NRI received from UE during initial PS network node selection to SGSN point code through NRI range mapping over Iu-Flex interface.
This configuration is used during initial PS core network node selection when the network resource identifier (NRI) from the UE is available. The NRI range is mapped to SGSN point code. This configuration is used when the core network uses Iu-Flex interface.
The command can be entered more than once to map multiple NRI ranges to same SGSN point code.
It is possible to configure multiple ranges to more than one SGSN however this configuration is required only when the PS core network is configured as Multi-Operator Core Network (MOCN).
When the PS core network is not MOCN and one range is mapped to more than one SGSN then SGSN is selected randomly in a non-predictable manner.

Example

The following command maps the NRI range from *101* to *201* with SGSN point code *1.2.3*:

```
map nri range 101 to 201 point-code 1.2.3
```

The following command maps the NRI range from *301* to *399* with SGSN point code *1.2.3*:

```
map nri range 301 to 399 point-code 1.2.3
```

The following command removes all NRI range matching entries between *301* to *399* from the configuration:

```
no map nri range 301 to 399
```

nri length

Configures the network resource identifier (NRI) length in bits to identify a specific SGSN serving in a pooled area. At least one NRI value must be assigned to an SGSN serving in a pool. The NRI is coded inside of the temporary mobile subscriber identity (TMSI), located within bits 14 to 23 with a variable length between 0 and 10 bits. The operator must set this NRI length to indicates the number of bits that shall be used for the NRI field to set the parameters for Iu-Flex (SGSN pooling) functionality.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

nri length *nri_value*

default nri length

default

Sets the NRI length to default value of 0 and disables the Iu-Flex (SGSN pooling) functionality.

nri length *nri_length*

Default: 0
Specifies the number of bits to be used in the P-TMS (bits 23 to 18) to define the network resource identifier (NRI). The NRI length configuration also sets the maximum size of the pool. If not configured, the NRI length is set to zero length.
length is an integer from 1 to 10. When a non-zero value is configured the PS network is considered to be a pool. Default: 0

Usage

Use this command to enable the Iu-Flex functionality on HNB-GW. This command identifies a unique SGSN serving a pooled area for Iu-Flex functionality and at least one NRI value has to assigned to an SGSN serving in a pool. It performs SGSN pooling/offloading scenario over Iu-Flex interface. The NRI is stored in the bits 14 to 23 of TMSI. The HNB-GW uses a portion of this NRI to set the parameters for Iu-Flex (SGSN pooling) functionality.
If more than one NRI is configured, the HNB-GW service does round-robin between the available NRIs when new subscriber(s) (re)connect.
This command must be used in conjunction with **null nri** command to configured SGSN pooling/offloading over Iu-Flex interface.

Example

The following command sets the HNB-GW to use bit length as *6* to derive the values from the NRI field (stored in the bits 14 to 23 of TMSI) to set the parameters for Iu-Flex (SGSN pooling) functionality:

```
nri length 6
```

null-nri

Configures the null network resource identifier (NRI) for load redistribution in support of Iu-Flex functionality. The NRI value defined with this command must be unique across the pool areas. This null-NRI is used by HNB-GW for load redistribution during SGSN offloading.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

null-nri *null_nri_value*

no null-nri *null_nri_value*

no

Disables/removes the configured null-NRI value used for SGSN offloading procedure.

null_nri_value

Indicates the null-NRI value to be used by HNB-GW for load re-distribution during SGSN offloading as an integer from 0 through 1023.
Without MOCN configuration this value can be entered only once.For MOCN a unique null-NRI must be assigned to each MOCN operator identify by its PLMN-ID (MCC+MNC).
A 0 (zero) value configured as null-NRI indicates the keyword is not to be used. There is no default value for this parameter.

Usage

Use this command to identify the SGSN by HNB-GW to be used for load redistribution during SGSN offloading over Iu-Flex interface.
There is one unique null-NRI in a PLMN supporting pool functionality.
Without MOCN configuration this command can be entered only once. In case of MOCN a unique null-NRI must be assigned to each MOCN operator identify by its PLMN-id (MCC+MNC).

Example

The following command sets the null-NRI as *1001* to be used by HNB-GW for load redistribution during SGSN offloading:

```
null-nri 1001
```

offload-sgsn

Enables or disables the exclusion of a specified primary SGSN node during the NAS Node Selection Function (NNSF) procedure when it needs to be offloaded using Iu-Flex functionality.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

[no] offload-sgsn point-code *sgsn_point_code*

no

Removes the specified primary SGSN point code from the exclusion list for NNSF function on HNB-GW and re-enables the inclusion of the primary SGSN node to be considered by HNB-GW.

point-code *sgsn_point_code*

Specifies SS7 address of primary SGSN in PS network having specific point code value to be excluded for NNSF function on HNB-GW when it needs to be offloaded in Iu-Flex functionality.
point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.
Only one instance of this primary SGSN point code can be mapped with one PS core network id.

Usage

Use this command to provision the HNB-GW to enable or disable the exclusion of the SGSN node when it needs to be offloaded.
When this command is enabled for exclusion of SGSN node during NNSF function in HNB-GW, the HNB-GW excludes the particular node from being considered.
User can re-enable the inclusion of the SGSN node to be considered for NNSF functionality by **no offload-sgsn point-code** command.

Important: The offload check is only for the primary point code and NOT for the backup point code.

This command can be used for planned maintenance as well.

Example

The following command configures the HNB-GW to exclude the primary SGSN point code *1.2.3* from being considered in NSSF function for Iu-Flex support:

```
offload-sgsn point-code 1.2.3
```

The following command re-enables the inclusion of SGSN point code *1.2.3* from being considered in NSSF function for Iu-Flex support:

```
no offload-sgsn point-code 1.2.3
```

sgsn deadtime

Configures a timer on HNB-GW to manage SGSN availability in a PS core network on receiving of a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

sgsn deadtime { immidiate |*dur* }

[no | default] sgsn deaddtime

no

Makes the peer node (SGSN) always available for all HNB-PS network instances.

default

Sets the default action for HNB-GW such that the peer node (SGSN) is marked down as soon as HNB-GW receives a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP in a specific HNB-PS network instance. Default: Enabled

immidiate

Sets the HNB-GW to mark the peer node (SGSN) down immediately and clears all Iu-PS connections towards the SGSN. Default: Disabled

dur

Sets the duration (in seconds) for a timer which starts once HNB-GW receives a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer SGSN. On expiry of this timer the peer SGSN is marked as dead and all Iu-PS connections towards that SGSN are released.
dur is tan integer from 1 through 30.
Only one instance of this command can be configured.

Usage

This command is used to configure a timer on HNB-GW to manage SGSN availability in a PS core network on receiving of PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP.
Timer value sets the duration in seconds for a timer which started once HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer SGSN. On expiry of this timer the peer SGSN is marked as dead and all Iu-PS connections towards that SGSN shall be released.

Important: This command can be entered only once. Reentering this command overwrites the previous parameters.

Example

The following command configures the deadtime timer value for *10* seconds on HNB-GW. Once HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer SGSN the HNB-GW waits for configured period and on expiry of timer it marks the specific SGSN as dead:

```
sgsn deadtime 10
```

sgsn point-code

Configures the default SGSN point-code with the HNB-PS network instance. This command is used when HNB-GW is to be connected to only one SGSN with in a PS network or as the default SGSN for all HNBs connected through specific HNB-PS network instance.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

`[ no ] sgsn point-code` *`point_code`*

`no`

Removes the configured default SGSN point code from specific HNB-PS network instance.

Caution: Removing the SGSN point code is a disruptive operation and affects all HNB sessions which are connected to particular SGSN through an HNB-PS network instance.

`point_code`

Specifies the SS7 address of the default SGSN in a PS network.
`point_code` is ann SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.
Only one instance of this command can be configured.

Usage

Use this command to configure a default SGSN to which HNB connects for PS network access through the HNB-GW service.
Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC Range.
- a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

Important: This command can be entered only once. If entered again the previous value shall be overwritten.

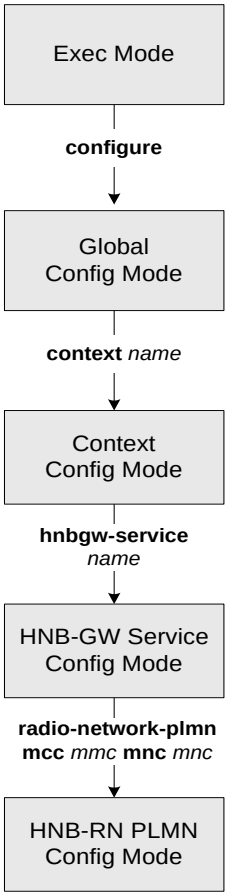
Example

The following command configures a default SGSN with point code *`101.201.101`* for HNBs to access PS network through HNB-GW service in this HNB-PS network instance:

```
sgsn point-code 101.201.101
```

Chapter 147
HNB-RN PLMN Configuration Mode Commands

This HNB Radio Network PLMN configuration mode defines the radio network PLMN parameters related to the HNB-GW connection with a UMTS Femto radio network.



associate cs-network

Associates a preconfigured circuit switched (CS) network within an HNB radio network PLMN with HNB-GW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] associate cs-network cs_name [ lac lac]
```

no

Disassociates/removes the configured CS network with an HNB radio network PLMN.

cs_name

Specifies the name of a preconfigured CS network in Global Configuration mode to be associated with an HNB radio network PLMN.
To configure CS network, refer to the *HNB-CS Configuration Mode Commands* chapter.

lac *lac_id*

Defines the granularity level of the circuit switch network to a location area code (LAC) level as an integer from 1 and 65535.

Usage

Use this command to associate pre-defined CS networks with a radio network PLMN in an HNB-GW service.
The circuit switched network comprises of one or more MSCs, where CS-domain IU-connections shall be routed. In a typical deployment HNB-GW is connected to only one MSC. However due to Iu-flex and networks-sharing requirements, HNB-GW can be connected to more than one MSCs as well.
Another scenario when HNB-GW can be connected to multiple MSCs is when a set of HNBs should be connected to a particular MSC based on their UTRAN location or geographical location.
This command provides configuration to have one or more MSCs such that these are used in load-shared (IuFlex) or network-shared mode. If location based distribution of HNBs to MSCs is desired, more than one circuit switched network configuration will be required.
This configuration allows association of a circuit switched network with a radio network PLMN and granularity can either be at the PLMN level or at the level of a location area (LAC) in that PLMN.
To configure CS network, refer to the *HNB-CS Configuration Mode Commands* chapter.

Example

The following command associates a CS network *umts1* with radio network PLMN with a granularity of LAC *234*:

```
associate cs-network umts1 lac 234
```

associate ps-network

Associates a preconfigured packet switched (PS) network within an HNB radio network PLMN with HNB-GW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

[no] associate ps-network *ps_name* **[lac** *lac* **[rac** *rac* **]]**

no

Disassociates/removes the configured PS network with an HNB radio network PLMN configured in HNB-GW service mode.

ps_name

Specifies the name of a preconfigured PS network to be associated with an HNB radio network PLMN configured in HNB-GW service mode.
To configure the PS network, refer to the *HNB PS Configuration Mode Commands* chapter.

lac *lac_id*

Specifies the granularity level of the packet switched network to a location area code (LAC) level as an integer from 1 and 65535.

rac *rac_id*

Specifies the granularity level of the packet switched network to a radio area code (RAC) level expressed as an integer from 1 and 65535.

Usage

Use this command to associate pre-defined PS networks with HNB radio network PLMN in an HNB-GW service.
The packet switched network comprises of one or more SGSNs where PS-domain IU-connections shall be routed. In a typical deployment HNB-GW is connected to only one SGSN. However with IuFlex and network-sharing functionality, HNB-GW can be connected to more than one SGSNs as well.
Another scenario when HNB-GW can be connected to multiple SGSNs is when a set of HNBs should be connected to a particular SGSN based on their UTRAN location or geographical location.
This command provides configuration to have one or more to have one or more SGSNs such that these are used in load-shared (iu-flex) or network-shared mode. If location based distribution of HNBs to SGSNs is desired then more than one packet switched network configuration will be required.
This command allows association of a packet switched network with a radio network PLMN and granularity could either be at the PLMN level or at the level of a location area code (LAC) in that PLMN or at the level of a routing area code (RAC) in that LAC.
To configure PS network, refer *HNB-PS Configuration Mode Commands* chapter.

Example

The following command associates a PS network *umts_ps1* with radio network PLMN with a granularity of LAC *234* and RAC as 123:

```
associate ps-network umts_ps1 lac 234 rac 123
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

rnc-id

Configures the Radio Network Concentrator (RNC) identifier in a Radio Network PLMN associated with HNB-GW service. The RNC identifier is provided to the HNB during HNB-REGISTRATION.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax

[no] rnc-id *rnc_id* **[lac** *lac_id* **[rac** *rac_id* **| cell-id** *cell_id* **]]**

no

Deletes the LAC and RAC information from the system configuration.

rnc-id

Specifies the RNC identifier as an integer from 1 through 65535.

lac *lac_id*

Specifies the granularity for the location of HNB to a location area code (LAC) and configures the RNC ID for all HNBs operating in particular location-area.
lac_id is an integer from 1 through 65535.

rac *rac_id*

Specifies the granularity level for the location of HNB as a routing area code (RAC) and configures the NC ID for all HNBs operating in particular routing area.
rac_id is an integer from 1 through 65535.

cell-id *cell_id*

Specifies the granularity for the location of HNB to a UTRAN cell level and configures RNC ID for all HNBs operating in particular UTRAN cell area.
cell_id is an integer from 1 through 65535.

Usage

Use this command to configure RNC id for Radio Network PLMN which will be sent to HNBs from HNB-GW during HNB-REGISTRATION procedure. Depending upon the requirement the RNC Identifier can be provided at the desired granularity.
When HNB-REGISTRATION request is received the RNC Id is looked up by matching the parameters received in the request. The most specific entry that matches the request shall have the highest priority, for example in the following configuration:

```
rnc-id 257 lac 1 cell-id 3

rnc-id 258 lac 1 rac 2
```

```
rnc-id 259 lac 1

rnc-id 260
```

- If the request is received with LAC=1, RAC=2, and Cell-Id=3, the selected RNC id will be 257.
- If the request is received with LAC=1, RAC=3, and Cell-Id = 3, the selected RNC id will be 258.
- If the request is received with LAC=1 and any other values of RAC and Cell-id, the selected RNC id will be 259. For all other requests 260 will be returned.

Example

The following command configures the HNB-GW service to return an RNC identifier as *102* when an HNB-REGISTRATION request is received with LAC *1*, and RAC *2*:

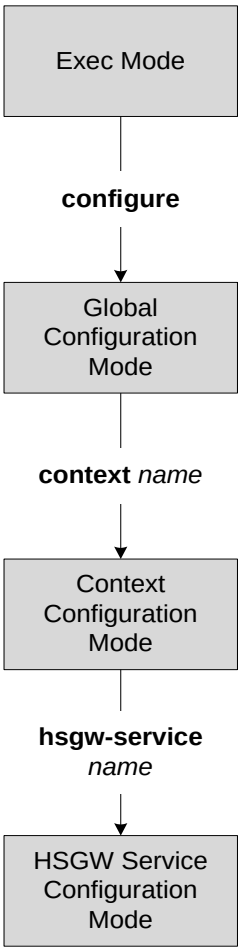
```
rnc-id 102 lac 1 rac 2
```

The following command configures the HNB-GW service to return an RNC identifier as *102* when an HNB-REGISTRATION request is received with LAC *1* and cell-id *4*:

```
rnc-id 102 lac 1 cell-id 5
```

Chapter 148
HSGW Service Configuration Mode Commands

The HSGW Service Configuration Mode is used to create and manage a configuration allowing the HRPD Serving Gateway (HSGW) to communicate, send and receive call data, and session flows to/from a evolved Access Network/evolved Packet Control Function (eAN/ePCF) in an eHRPD network.



a11-signalling-packets

Enables the DSCP marking feature for IP headers carrying outgoing A11-signalling A11 packets (such as RRP, RU, SU).

Product

HSGW

Privilege

Administrator

Syntax

a11-signalling-packets ip-header-dscp *value*

[default | no] a11-signalling-packets ip-header-dscp

default

Restores the specified parameter to its default setting of 0x0.

no

Disables the specified functionality.

ip-header-dscp *value*

Configures the QoS Differentiated Services Code Point (DSCP) marking for IP header encapsulation. *value*: Represents the DSCP setting as the first six most-significant bits of the ToS field. It can be configured to any hex value from 0x0 through 0x3F. Default is 0x0.

Usage

Use this command to enable or disable the DSCP marking feature for IP headers carrying outgoing A11-signalling A11 packets. DSCP marking is disabled by default.

Example

The following command configures the HSGW service to support DSCP marking for IP headers on A11 packets in outgoing A11-signalling traffic:

```
a11-signalling-packets ip-header-dscp 0x21
```

associate

Associates accounting policies and QCI-QoS mapping parameters with this HSGW service.

Product

HSGW

Privilege

Administrator

Syntax

associate { accounting-policy *name* **| qci-qos-mapping** *name* **}**

no associate { accounting-policy [*name* **] | qci-qos-mapping }**

no

Removes the specified associated policy or mapping from the service.

accounting-policy *name*

Specifies an existing accounting policy to associate with the HSGW service as an alphanumeric string of 1 through 63 characters.

qci-qos-mapping *name*

Specifies an existing QCI-QoS mapping configuration as an alphanumeric string of 1 through 63 characters. QCI-QoS mapping is configured through the **qci-qos-mapping** command in the Global Configuration Mode.

Usage

Use this command to associate an accounting policy with the HSGW service.

Example

The following command associates an accounting policy named *acct2* to the HSGW service:

```
associate accounting-policy acct2
```

bind address

Binds the service to a logical IP interface serving as the A10 interface and specifies the maximum number of subscribers that can access this service over the configured interface.

Product

HSGW

Privilege

Administrator

Syntax

bind address *ip_address* **[max-subscribers** *num* **]**

no bind address

no

Removes the interface binding from this service.

address *ip_address*

Specifies the IP address of the A10/A11 interface in IPv4 dotted-decimal notation.

max-subscribers *num*

Specifies the maximum number of subscribers that can access this service on this interface as an integer from 0 through 2500000. Default: 2500000

Important: The maximum number of subscribers supported is dependant on the license key installed and the number of active PSCs in the system. A fully loaded system with 13 active PSCs can support 3,000,000 total subscribers. Refer to the license key command and the Usage section (below) for additional information.

Usage

Associate the HSGW service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an A10/A11 interface that provides the session connectivity to/from an eAN/PCF. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.
This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.
When configuring the **max-subscribers** option, be sure to consider the following:

- The total number of A10/A11 interfaces you will configure
- The total number of subscriber sessions that all of the configured interfaces may handle during peak busy hours
- An average bandwidth per session multiplied by the total number of sessions
- The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

Example

The following command would bind the logical IP interface with the address of *112.334.556.778* to the HSGW service and specifies that a maximum of *200,000* simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 112.334.556.778 max-subscribers 200000
```

context-retention-timer

Configures the maximum number of consecutive seconds that a UE session context (which includes the LCP, authentication and A10 session context for a given UE) is maintained by the HSGW before it is torn down.

Product

HSGW

Privilege

Administrator

Syntax

context-retention-timer timeout [*sec* **]**

[default | no] context-retention-timer timeout

default

Disables the timer.

no

Disables the timer.

timeout [*sec* **]**

Specifies the amount of time (in seconds) that the session context is maintained before it is disassembled as an integer from 1 through 3600. Default: 60

Usage

Use this command to configure a timer to retain session contexts for a specified amount of time before disassembling it.

Example

The following command allows the HSGW to maintain session contexts for *120* seconds before tearing them down:

```
context-retention-timer timeout 120
```

data-available-indicator

Enables sending the Data Available Indicator extension in A10/A11 Registration Reply messages.

Product

HSGW

Privilege

Administrator

Syntax

```
data-available-indicator
```

Usage

Use this command to enable the sending of the Data Available Indicator extension in A10/A11 Registration Reply messages.

data-over-signaling

Enables the data-over-signaling marking feature for A10 packets.

Product

HSGW

Privilege

Administrator

Syntax

```
[ default | no ] data-over-signaling
```

default

Enables the data-over signaling feature for A10 packets.

no

Disables the data-over signaling feature for A10 packets.

Usage

Use this command to enable or disable the data-over signaling feature for A10 packets.

dns-pgw

Identifies the location of the DNS client to the HSGW service. The DNS client is used to identify an FQDN for the peer P-GW. This command defaults to the same context as the HSGW service.

Product

HSGW

Privilege

Administrator

Syntax

dns-pgw context *name*

[default | no] dns-pgw context

default

Returns the command to its default setting of the current context.

no

Removes the configured DNS client context name from this service.

context *name*

Specifies an existing context in which the DNS client is configured as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to identify to the HSGW service the context where the DNS client is configured.

Example

The following command identifies the context where the DNS client is configured as *isp3*:

```
dns-pgw context isp3
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

fqdn

Configures the Fully Qualified Domain Name (FQDN) for this HSGW service.

Product

HSGW

Privilege

Administrator

Syntax

fqdn *domain_name*

[default | no] fqdn

default

Returns the command to the default setting of "null".

no

Removes the configured FQDN name from this service.

domain_name

Specifies an FQDN for the HSGW service as an alphanumeric string of 1 through 256 characters.

Important: In order to properly interact with other nodes in the network, the FQDN should be 96 alpha and/or numeric characters or less.

Usage

Use this command to configure an FQDN for this HSGW service. The FQDN is used when matching a P-GW with an HSGW.

Topology Matching

You may specify which P-GW you wish an HSGW interface to connect with by enabling topology matching within the FQDNs for both the HSGW service and P-GW service. Topology matching selects geographically closer nodes and reduces backhaul traffic for a specified interface.

The following optional keywords enable or disable topology matching when added to the beginning of an FQDN:

- **topon**.<*interface_name*>.

  Beginning an FQDN with **topon** initiates topology matching with available P-GWs in the network. Once this feature is enabled, the rest of the FQDN is processed from right to left until a matching regional designator is found on a corresponding P-GW FQDN.

- **topoff**.<*interface_name*>.

  By default, topology matching is disabled. If you enable topology matching for any interfaces within a node, however, all interfaces not using this feature should be designated with **topoff**.

Example

The following command configures this HSGW service with an FQDN of *abc123.com*:

```
fqdn abc123.com
```

The following command configures this HSGW service with an FQDN that enables topology matching:

```
fqdn topon.<interface_name>.hsgw01.bos.ma.node.epc.mnc<value>.
mcc<value>.3gppnetwork.org
```

Important: The associated P-GW service must have a corresponding FQDN similar to the following:

```
topon.<interface_name>.pgw01.bos.ma.node.epc.mnc<value>.mcc<value>.3gppne
twork.org
```

fragment

Enables or disables Point-to-Point Protocol (PPP) payload fragmentation.

Product

HSGW

Privilege

Administrator

Syntax

```
[ default | no ] fragment ppp-data
```

default

Returns the command to its default setting of enabled.

no

Disables PPP payload fragmentation.

Usage

Use this command to enable or disable PPP payload fragmentation.

gre

Configures Generic Routing Encapsulation (GRE) parameters for the A10 protocol within the HSGW service.

Product

HSGW

Privilege

Administrator

Syntax

gre { checksum | checksum-verify | flow control [action { disconnect-session | resume-session }] [timeout *msecs* **] + | ip-header-dscp** *value* **{ all-control-packets | setup-packets-only } | reorder-timeout** *msecs* **| segmentation | sequence-mode { none | reorder } | sequence-numbers | threegppp2-ext-headers qos-marking }**

default gre { checksum | checksum-verify | flow-control | ip-header-dscp | reorder-timeout | sequence-mode | sequence-numbers | threegppp2-ext-headers qos-marking }

no gre { checksum | checksum-verify | flow-control | ip-header-dscp | segmentation | sequence-numbers | threegppp2-ext-headers qos-marking }

default

Restores the specified parameter to its default setting.

no

Disables the specified functionality.

checksum

Enables the introduction of the checksum field in outgoing GRE packets. Default: disabled

checksum-verify

Enables verification of the GRE checksum (if present) in incoming GRE packets. Default: disabled

flow-control [action { disconnect-session | resume-session }] [timeout *msecs* **] +**

Default: no GRE flow-control
Enables 3GPP2 GRE flow control which causes the HSGW to send flow control enabled Normal Vendor Specific Extensions (NVSE) in A11 RRPs.

action { disconnect-session | resume-session }:
Default: disconnect-session
Specifies the action to be taken when timeout is reached:

- **disconnect-session**: Ends the session and releases the call.
- **resume-session**: Switches flow control to XON and resumes delivery of packets to the RAN.

timeout *msecs*
Specifies the amount of time (in milliseconds) to wait for an XON indicator from the RAN (after receiving an XOFF). Also sets the action to be taken if the timeout limit is reached.

msecs is an integer from 1 through 1000000. Default: 1000

ip-header-dscp *value* **{ all-control-packets | setup-packets-only }**

Default: Disabled
Configures QoS Differentiated Services Code Point (DSCP) marking for GRE packets.

- *value*: Represents the DSCP setting as the first six most-significant bits of the ToS field. It can be configured to any hexadecimal value from 0x0 through 0x3F.
- **all-control-packets**: Dictates that the DSCP marking is to be provided in all GRE control packets.
- **setup-packets-only**: Dictates that the DSCP marking is to be provided only in GRE setup packets.

reorder-timeout *msecs*

Configures the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets as an integer from 0 through 5000. Default: 100

segmentation

Enables GRE Segmentation for the HSGW service. Default: disabled

sequence-mode { none | reorder }

Default: none
Configures handling of incoming out-of-sequence GRE packets.
none: Specifies that sequence numbers in packets are ignored and all arriving packets are processed in the order they arrive.
reorder: Specifies that out of sequence packets are stored in a sequencing queue until one of the conditions is met:

- The reorder timeout occurs: All queued packets are sent for processing and the accepted sequence number is updated to the highest number in the queue.
- The queue is full (five packets): All packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number in the queue.
- An arriving packet has a sequence number such that the difference between this and the packet at the head of the queue is greater than five. All the packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number that arrived.
- A packet arrives that fills a gap in the sequenced numbers stored in the queue and creates a subset of packets whose sequence numbers are continuous with the current accepted sequence number. This subset of packets in the queue is sent for processing. The reorder timer continues to run and the accepted sequence number is updated to the highest number in the subset delivered.

sequence-numbers

Enables insertion of GRE sequence numbers in data that is about to be transmitted over the A10 interface. Data coming into the system containing sequence numbers but that is out of sequence is not re-sequenced.

threegppp2-ext-headers qos-marking

When threegppp2-ext-headers qos-marking is enabled and the PCF negotiates capability in the A11 RRQ, the HSGW will include the QoS optional data attribute in the GRE 3gpp2 extension header.
The **no** keyword, enables qos-marking in the GRE header based on the tos value in the header.

Usage

Use this command to set GRE parameters for the A10 protocol within the HSGW service.

Example

The following command configures the HSGW service to support the inclusion of GRE sequence numbers in outgoing traffic:

```
gre sequence-numbers
```

ip

Enables the use of Robust Header Compression (RoHC) and enters the HSGW Service ROHC Configuration Mode where RoHC parameters are configured for the service.

Configures the local User Datagram Protocol (UDP) port for the A10/A11 interface IP socket.

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network. Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

Product

HSGW

Privilege

Administrator

Syntax

ip { header-compression rohc | local-port *number* **| source-violation { clear-on-valid-packet | drop-limit** *num* **| period** *secs* **| reneg-limit** *num* **} }**

default ip { header-compression rohc | local-port | source-violation { drop-limit | period | reneg-limit } }

no ip { header-compression rohc | source-violation clear-on-valid-packet }

default

Resets the keyword to its default value.

no

header-compression rohc: Removes the RoHC configuration from this service.
ip source-violation clear-on-valid-packet: Disables the ability of the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

header-compression rohc

Specifies that Robust Header Compression will be applied to sessions using this service and enters the HSGW Service RoHC Configuration Mode where RoHC parameters are configured.

local-port *number*

Specifies the UDP port number as an integer from 1 through 65535. Default: 699

source-violation { clear-on-valid-packet | drop-limit *num* **| period** *secs* **| reneg-limit** *num* **}**

clear-on-valid-packet
Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet. Default: disabled
drop-limit *num*
Specifies the number of allowed source violations within a detection period before forcing a call disconnect as an integer from 1 through 1000000. If *num* is not specified, the value is set to the default. Default: 10
period *secs*

Specifies the length of time (in seconds) for a source violation detection period to last; drop-limit and reneg-limit counters are decremented each time this value is reached.
The counters are decremented in this manner: reneg-limit counter is reduced by one (1) each time the period value is reached until the counter is zero (0); drop-limit counter is halved each time the period value is reached until the counter is zero (0). If *secs* is not specified, the value is set to the default.
secs is an integer from 1 through1000000. Default: 120

reneg-limit *num*

Sets the number of allowed source violations within a detection period before forcing a PPP renegotiation. If *num* is not specified, the value is set to the default.
num is an integer from 1 through 1000000. Default: 5

Usage

Header Compression RoHC: Use this command to specify that sessions using this service will have Robust Header Compression applied and configure parameters supporting RoHC.
Entering this command results in the following prompt:

```
[context_name]hostname(config-ip-header-compression-rohc)#
```

HSGW Service RoHC Configuration Mode commands are defined in the HSGW Service RoHC Configuration Mode Commands chapter.
Local Port: Specify the UDP port that should be used for communications between the Packet Control Function (PCF) and the HSGW.

Important: The UDP port setting on the PCF must match the local-port setting for the HSGW service on the system in order for the two devices to communicate.

Source Violation: This function is intended to allow the operator to configure a network to prevent problems such as when a user gets handed back and forth between two HSGWs a number of times during a handoff scenario.
This function operates in the following manner:
When a subscriber packet is received with a source address violation, the system increments both the IP source-violation reneg-limit and drop-limit counters and starts the timer for the IP-source violation period. Every subsequent packet received with a bad source address during the IP-source violation period causes the reneg-limit and drop-limit counters to increment.
For example, if reneg-limit is set to 5, then the system allows 5 packets with a bad source address (source violations), but on the 5th packet, it re-negotiates PPP.
If the drop-limit is set to 10, the above process of receiving 5 source violations and renegotiating PPP occurs only once. After the second 5 source violations, the call is dropped. The period timer continues to count throughout this process.
If the configured source-violation period is exceeded at any time before the call is dropped, the reneg-limit counter is checked. If the reneg-limit counter is greater than zero (0), the reneg-limit is decremented by 1. If the reneg-limit counter equals zero, the drop-limit is decremented by half.

Example

The following command specifies a UDP port of 3950 for the HSGW service to use to communicate with the PCF on the A10/A11 interface:

```
ip local-port 3950
```

The following command sets the drop limit to *15* and leaves the other values at their defaults:

```
ip source-violation drop-limit 15
```

lifetime

Specifies how long an A10 connection can exist before its registration is considered expired.

Product

HSGW

Privilege

Administrator

Syntax

lifetime *time*

[default | no] lifetime

default

Resets the lifetime value to the default setting of 1800 seconds.

no

Specifies that an A10 connection can exist for an infinite amount of time.

time

Specifies the time (in seconds) that an A10 connection can exist before its registration is considered expired as an integer from 1 through 65534. Default: 1800

Usage

Use this command to set a limit to the amount of time that a subscriber session can remain up whether or not the session is active or dormant. If the lifetime timer expires before the subscriber terminates the session, the connection is terminated automatically.

Example

The following command specifies a time of *3600* seconds (1 hour) for subscriber sessions on this HSGW service:

```
lifetime 3600
```

max-retransmissions

Configures the maximum number of times the HSGW service will attempt to communicate with an eAN/PCF before it marks it as unreachable.

Product

HSGW

Privilege

Administrator

Syntax

max-retransmissions *count*

default max-retransmissions

default

Resets the maximum number of allowed retransmissions to the default value of 5.

count

Specifies the maximum number of times the HSGW service will attempt to communicate with an eAN/PCF before it marks it as unreachable.
count is an integer from 1 through 1000000. Default: 5

Usage

Use this command to limit the number of retransmissions to an eAN/PCF before marking it as unreachable. If the value configured is reached, the call is dropped.

Example

The following command configures the maximum number of retransmissions for the HSGW service to *3*:

```
max-retransmissions 3
```

mobile-access-gateway

Identifies the mobile access gateway (MAG) context through which MIPv6 calls are to be routed.

Product

HSGW

Privilege

Administrator

Syntax

```
mobile-access-gateway context context_name [ mag-service service_name ]

no mobile-access-gateway context
```

no

Removes the configured MAG context route from this service.

context *context_name* **[mag-service** *service_name* **]**

Specifies the name of the context and, optionally, the service through which MIPv6 sessions are to be routed. *context_name* is an existing context expressed as an alphanumeric string of 1 through 79 characters. *service_name* is an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify where MIPv6 sessions are routed through this service.

Example

The following command identifies the MAG context *MAG1* as the context through which MIPv6 sessions are to be routed and further narrows the route by specifying the service name (*mag_serv3*):

```
mobile-access-gateway context MAG1 mag-service mag_serv3
```

network-initiated-qos

Enables the use of network initiated QoS functionality.

Product

HSGW

Privilege

Administrator

Syntax

```
[ default | no ] network-initiated-qos
```

default

Returns the command to its default setting of enabled.

no

Disables the ability to use network initiated QoS functionality.

Usage

Use this command to enable or disable support for network initiated QoS functionality. Network initiated QoS is enabled by default.
When network initiated QoS functionality is enabled, if the vendor specific network control protocol (VSNCP) protocol configuration options (PCO) arrive from the UE with the BCM set, the HSGW CCR-I includes the Network-Request-Support AVP. If the PCRF behavior returns a BCM of MS+NW when this AVP is received, then flows originating from the network (RSVP Resv) would be triggered upon a PCC-Rule install.

plmn id

Configures Public Land Mobile Network identifiers used to determine if a mobile station is visiting, roaming or belongs to this network.

Product

HSGW

Privilege

Administrator

Syntax

plmn id mcc *number* **mnc** *number*

mcc *number* **mnc** *number*

mcc *number*: Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer fromn 100 through 999.
mnc *number*: Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

Usage

The PLMN identifier is used to aid the HSGW service in the determination of whether or not a mobile station is visiting, roaming, or home. Multiple P-GW services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each P-GW Service. The configured IDs are used in Diameter-EAP-Request messages (as a Visited-Network-Identifier AVP).

Example

The following command configures the PLMN identifier with an MCC of *462* and MNC of *2*:

```
plmn id mcc 462 mnc 02
```

policy overload

Specifies how an HSGW service should handle overload conditions.

Product

HSGW

Privilege

Administrator

Syntax

policy overload { redirect *address* **[weight** *weight_num* **] [** *address2* **[weight** *weight_num* **] ... address16 [weight** *weight_num* **]] | reject [use reject-code { admin-prohibite | insufficient-resources }] }**

default policy overload

no policy overload [redirect *address* **[** *address2* **] ... [** *address16* **]**

default

Returns the command to it default setting of "reject" with the "admin-prohibited" code.

no

Removes a specified "redirect address" from this service.

redirect *address* **[weight** *weight_num* **] [** *address2* **[weight** *weight_num* **] ...** *address16* **[weight** *weight_num* **]]**

This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the HSGW service rejects new sessions with an A11 Registration Reply Code of 88H (unknown HSGW address) and provides the IP address of an alternate HSGW. This command can be issued multiple times.
address: The IP address of an alternate HSGW expressed in IPv4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.
weight *weight_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified, the entry is automatically assigned a weight of 1 (default). *weight_num* must be an integer value from 1 through 10.

reject [use reject-code { admin-prohibite | insufficient-resources }]

This option will cause any overload traffic to be rejected. The HSGW sends an A11 Registration Reply Code of 82H (insufficient resources).
use-reject-code admin-prohibited: When this keyword is specified and traffic is rejected, the error code admin prohibited is returned instead of the error code "insufficient resources". This is the default behavior.
use-reject-code insufficient-resources: When this keyword is specified and traffic is rejected, the error code "insufficient resources" is returned instead of the error code admin prohibited.

Usage

Policies can be implemented to dictate HSGW service behavior for overload conditions.
The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system.
The system automatically invokes the overload policy when an on-line software upgrade is started.
Use the **no policy overload** command to delete a previously configured policy. If after deleting the policy setting you desire to return the policy parameter to its default setting, use the **default policy** command.
The chassis is shipped from the factory with the policy options overload disabled

Example

The following command configures the HSGW service to redirect overload traffic to two IPv4 addresses, one priority weighted *1* and the other priority weighted *5*:

```
policy overload redirect 10.2.3.4 weight 1 10.2.3.5 weight 5
```

profile-id-qci-mapping

Associates a configured mapping table for RP QoS Profile ID to LTE QoS Class Index (QCI) mapping with this service.

Product

HSGW

Privilege

Administrator

Syntax

profile-id-qci-mapping *name*

no profile-id-qci-mapping [*name* **]**

no

Removes all profile maps or a specific profile map from this service.

name

Specifies the name of an existing Profile ID - QCI Mapping table to be associated with this service as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to associate the HSGW service with a configured Profile ID - QCI Mapping table. The table is configured in the Global Configuration Mode using the **profile-id-qci-mapping-table** command.

Example

The following command associates a Profile ID - QCI Mapping table named *table3* with this service:

```
profile-id-qci-mapping table3
```

registration-deny

Configures parameters related to registration rejection.

Product

HSGW

Privilege

Administrator

Syntax

```
registration-deny { handoff connection-setup-record-absent | newcall connection-setup-record-absent } [ use-deny-code { poorly-formed-request | reason-unspecified } ]

[ default | no ] registration-deny { handoff connection-setup-record-absent | newcall connection-setup-record-absent }
```

default | no

Returns the command to its default settings.

handoff connection-setup-record-absent

When enabled, the HSGW denies or discards handoff R-P sessions that do not have an Airlink Connection Setup record in the A11 Registration Request.
Default is disabled. Default HSGW behavior is to accept such requests.

newcall connection-setup-record-absent

When enabled, the HSGW denies or discards new R-P sessions that do not have the Airlink Connection Setup record in the A11 Registration Request.
Default is disabled. Default HSGW behavior is to accept such requests.

use-deny-code { poorly-formed-request | reason-unspecified }

Sets the specified Registration Deny Code when denying a new call or handoff because of a missing connection setup record.

Usage

Use this command to configure parameters relating to the rejection of registration requests.

Example

The following command denies registration for registration requests missing the connection setup record and replies with a use deny code of “poorly formed request”:

```
registration-deny handoff connection-setup-record-absent use-deny-code poorly-formed-request
```

retransmission-timeout

Configures the maximum allowable time for the HSGW service to wait for a response from the eAN/PCF before it attempts to communicate with the eAN/PCF again (if the system is configured to retry the PCF), or marks the eAN/PCF as unreachable.

Product

HSGW

Privilege

Administrator

Syntax

retransmission-timeout *time*

[default | no] retransmission-timeout

default

Resets the timeout setting to the default value of 3.

no

Deletes a previously configured timeout value.

time

Specifies the maximum allowable time (in seconds) for the HSGW service to wait for a response from the eAN/PCF before it: a) attempts to communicate with the eAN/PCF again (if the system is configured to retry the PCF), or b) marks the eAN/PCF as unreachable.
time is an integer from 1 through 1000000. Default: 3

Usage

Use the retransmission timeout command in conjunction with the **max-retransmissions** command in order to configure the HSGW service's behavior when it does not receive a response from a particular PCF.

Example

The following command configures a retransmission timeout value of *5* seconds:

```
retransmission-timeout 5
```

rsvp

Configures resource reservation protocol (RSVP) parameters for this HSGW service in support of the network initiated QoS feature.

Product

HSGW

Privilege

Administrator

Syntax

```
rsvp { max-retransmissions count | retransmission-timeout seconds }

[ default | no ] rsvp { max-retransmissions | retransmission-timeout }
```

default

Resets the maximum number of allowed retransmissions to the default value of 5 or the timeout setting to the default value of 3.

no

Disables the feature.

max-retransmissions *count*

Specifies the maximum retransmission count of RP control packets as an integer from 1 through 1000000. Default: 5

retransmission-timeout *seconds*

Specifies the maximum amount of time (in seconds) to allow for retransmission of RP control packets as an integer from 1 through 1000000. Default: 3

Usage

Use this command to set RSVP parameters for this HSGW service in support of the network initiated QoS feature.

Example

The following command configures the maximum number of retransmissions to *3*:

```
rsvp max-retransmissions 3
```

setup-timeout

Specifies the maximum amount of time allowed for session setup.

Product

HSGW

Privilege

Administrator

Syntax

setup-timeout *seconds*

[default| no] setup-timeout

default

Resets the command to the default value of enabled with a timeout of 60 seconds.

no

Disables the feature.

seconds

Specifies the maximum amount of time (in seconds) to allow for setup of a session in this service as an integer from 1 though 1000000. Default: 60

Usage

Use this command to set the maximum amount of time allowed for setting up a session.

Example

The following command sets the maximum time allowed for setting up a session to 5 minutes (300 seconds):

```
setup-timeout 300
```

spi remote-address

Configures the security parameter index (SPI) between the HSGW service and the evolved Access Network/evolved Packet Control Function (eAN/ePCF). This command also configures the redirection of calls based on the PCF zone.

Product

HSGW

Privilege

Administrator

Syntax

```
spi remote-address { pcf_ip_address | ip_addr_mask_combo } spi-number number { encrypted
secret enc_secret | secret secret } [ description string ] [ hash-algorithm { md5 |
rfc2002-md5 } ] [ replay-protection { nonce | timestamp } ] [ timestamp-tolerance
tolerance ] [ zone zone_id ]

no spi remote-address pcf_ip_address spi-number number
```

pcf_ip_address **|** *ip_addr_mask_combo*

pcf_ip_address: Specifies the IP address of the ePCF. *pcf_ip_address* is an IP address expressed in IPv4 dotted decimal notation or IPv6 colon separated notation.
ip_addr_mask_combo: Specifies the IP address and mask bits of the PCF. *ip_addr_mask_combo* must be specified using the form "IP Address/Mask Bits" where the IP address must in IPv4 dotted-decimal or IPv6 colon-separated notation, and the mask bits are a numeric value corresponding to the number of bits in the subnet mask.

spi-number *number*

Specifies the SPI which indicates a security context between the PCF and the HSGW as an integer from 256 through 4294967295.

encrypted secret *enc_secret* **| secret** *secret*

Configures the shared-secret between the HSGW service and the PCF. The secret can be either encrypted or non-encrypted.
encrypted secret *enc_secret*: Specifies the encrypted shared key (*enc_secret*) between the PCF and the HSGW service. *enc_secret* must be between 1 and 236 alpha and/or numeric characters and is case sensitive.
secret *secret*: Specifies the shared key (secret) between the PCF and the HSGW services. *secret* must be between 1 and 127 alpha and/or numeric characters and is case sensitive.
The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

description *string*

This is a description for the SPI expressed as an alphanumeric string of 1 through 31 characters.

hash-algorithm { md5 | rfc2002-md5 }

Specifies the hash-algorithm used between the HSGW service and the PCF. Default: md5

md5: Configures the hash-algorithm to implement MD5.
rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5.

replay-protection { nonce | timestamp }

Specifies the replay-protection scheme that should be implemented by the HSGW service. Default: timestamp
nonce: Configures replay protection to be implemented using NONCE (Number ONCE).
timestamp: Configures replay protection to be implemented using timestamps.

timestamp-tolerance *tolerance*

Specifies the allowable difference (in seconds) between timestamps as an integer from 0 through 65535. If the difference is exceeded, the session will be rejected. If set to 0, timestamp tolerance checking is disabled at the receiving end. Default: 60

zone *zone_id*

Specifies the different PCF zones to configure in HSGW service. Mapping of a zone-number to a set of HSGWs can be done per HSGW service basis.
zone_id is an integer value from 1 through 32. A maximum of 32 PCF zones can be configured for a HSGW service.

Usage

An SPI is a security mechanism configured and shared by the PCF and the HSGW service. Please refer to *IETF RFC 2002: IP Mobility Support* for additional information.
Multiple SPIs can be configured if the HSGW service is communicating with multiple eAN/ePCFs.

Important: The SPI configuration on the PCF must match the SPI configuration for the HSGW service on the system in order for the two devices to communicate properly.

Example

This command used with the **zone** keyword redirects all calls on the basis of PCF zone to the specific HSGW on the basis of parameters configured using the **policy pcf-zone-match** command.

The following command configures the HSGW service to use an SPI of *256* when communicating with a PCF with the IP address *192.168.0.2*. The key that would be shared between the PCF and the HSGW service is *q397F65*.

```
spi remote-address 192.168.0.2 spi-number 256 secret q397F65
```

The following command creates the configured SPI of *400* for an PCF with an IP address of *172.100.3.200* and zone id as *11*:

```
spi remote-address 172.100.3.200 spi-number 400 zone 11
```

unauthorized-flows

Configures the service to wait a specified number of seconds before triggering a QoS update to downgrade an unauthorized flow.

Product

HSGW

Privilege

Administrator

Syntax

unauthorized-flows qos-update wait-timeout *seconds*

[default | no] unauthorized-flows qos-update wait-timeout

default

Returns the command to its default setting.

no

Removes the configure wait-timeout setting for this service.

qos-update wait-timeout *seconds*

Specifies the number of seconds to wait before triggering the QoS update to downgrade the unauthorized flow as an integer from 1 through 65534.

Usage

Use this command to specific a wait timeout trigger for flows that are unauthorized by policy rules received via the Gxa interface from the PCRF. When the wit timer expires, the HSGW triggers a QoS update to downgrade the unauthorized flow.

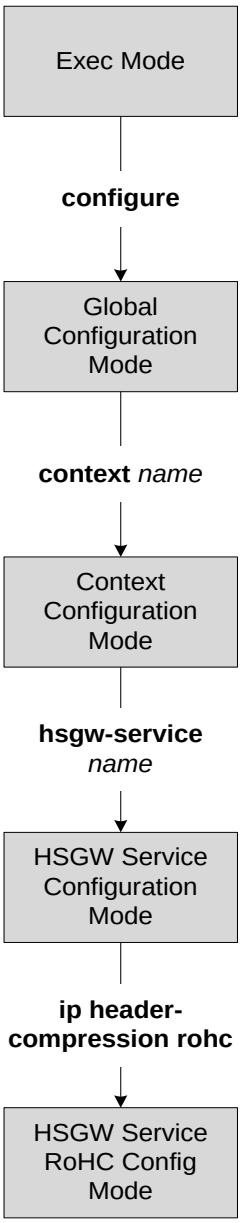
Example

The following command configures the HSGW service to apply the wait time of *30* seconds after receiving an flow unauthorized by the PCRF:

```
unauthorized-flow qos-update wait-timeout 30
```

Chapter 149
HSGW Service RoHC Configuration Mode Commands

The HSGW Service RoHC Configuration Mode is used to configure Robust Header Compression (RoHC) parameters for the service.



cid-mode

This mode allows you to configure options that apply during RoHC compression for the service.

Product

HSGW

Privilege

Administrator

Syntax

cid-mode { large | small } max-cid *integer*

default cid-mode

default

Reset all options in the RoHC Profile Compression Configuration mode to their default values.

large

Use large packets with optional information for RoHC

small

This is the default packet size.
Use small RoHC packets.

max-cid *integer*

Specifies the highest context ID number to be used by the compressor as an integer from 0 through 15 when small packet size is selected, and 0 through 31 when large packet size is selected. Default: 15

Usage

Use this command to set the RoHC packet size and define the maximum

Example

The following command sets large RoHC packet size and sets the maximum CID to *100*:

```
cid-mode large max-cid 100
```

The following command sets the cid-mode to the default settings of small packets and max-cid 0:

```
default cid-mode
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

mrru

Specifies the size of the largest reconstructed reception unit that the decompressor is expected to reassemble from segments. The size includes the CRC. If maximum received reconstructed unit (MRRU) is negotiated to be 0, no segment headers are allowed on the channel.

Product

HSGW

Privilege

Administrator

Syntax

mrru *num_octets*

default mrru

default

Resets the value of this command to its default setting of 0.

num_octets

Specifies the number of allowed octets for the MRRU as an integer from 0 through 65535. Default: 0

Usage

Use this command to set the size, in octets, of the largest reconstructed reception unit that the decompressor is expected to reassemble from segments.

Example

The following command sets the largest reconstructed reception unit to 1024 octets:

```
mrru 1024
```

The following command resets the MRRU size to its default of 0 octets:

```
default mrru
```

profile

Specifies the header compression profiles to use. A header compression profile is a specification of how to compress the headers of a specific kind of packet stream over a specific kind of link. At least one profile must be specified.

Product

HSGW

Privilege

Administrator

Syntax

```
profile { [ esp-ip ] [ rtp-udp ] [ udp-ip ] [ uncompressed-ip ] }

default profile
```

default

Default: esp-ip rtp-udp udp-ip uncompressed-ip
Returns the RoHC profile configuration to its default setting.

esp-ip

Enables RoHC Profile 0x0003 which is for ESP/IP compression, compression of the header chain up to and including the first ESP header, but not subsequent subheaders.

rtp-udp

Enables RoHC Profile 0x0001 which is for RTP/UDP/IP compression

udp-ip

Enables RoHC Profile 0x0002 which is for UDP/IP compression; compression of the first 12 octets of the UDP payload is not attempted.

uncompressed-ip

Enables RoHC Profile 0x0000 which is for sending uncompressed IP packets.

Usage

Use this command to specify the RoHC header compression profiles.

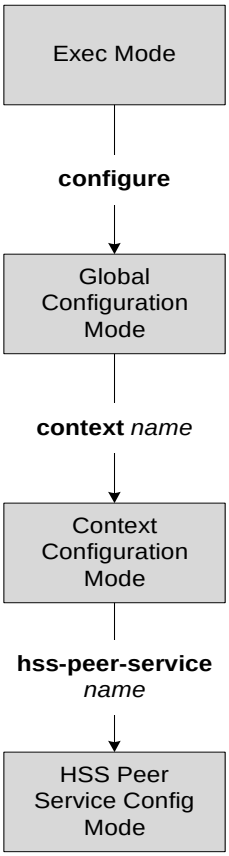
Example

The following command sets the profiles to use as *esp-ip* and *rtp-udp*:

```
profile esp-ip rtp-udp
```

Chapter 150
HSS Peer Service Configuration Mode Commands

The HSS Peer Service Configuration Mode is used to create and manage the Home Subscriber Server (HSS) Peer Service.



auth-request

Configures the number of authentication vectors the MME requests in an Authentication-Information-Request (AIR) message to the HSS for each UE requiring authentication.

Product

MME

Privilege

Administrator

Syntax

auth-request num-auth-vectors *num*

default auth-request num-auth-vectors

num-auth-vectors *num*

Specifies the number of vectors the MME is requesting from the HSS as an integer from 1 through 3. Default = 1

Usage

Use this command to configure the number of authentication vectors the MME requests in an Authentication-Information-Request (AIR) message to the HSS for each UE requiring authentication.
Receiving multiple vectors from the HSS for a given UE helps reduce the number of messages across the diameter connection plus provides the MME with additional vectors for the UE in the event that the connection or the HSS id disabled.
To view the current number of requested vectors, execute the **show hss-peer-service service name** <*name*> command in the Exec mode.

Example

The following command sets the number of requested vectors to 2:

```
auth-request num-auth-vectors 2
```

diameter hss-dictionary

Specifies the Diameter Credit Control dictionary for the HSS peer service.

Product

MME

Privilege

Administrator

Syntax

```
diameter hss-dictionary { custom1 | standard | standard-r9 } [ eir-dictionary { custom1 |
standard | standard-r9 } ]

default diameter hss-dictionary
```

default

Sets the dictionary to default **standard-r9** for HSS service.

custom1

Sets the Diameter dictionary to a customer-specific HSS Diameter dictionary. Default: Disabled

standard

Sets the Diameter dictionary to the standard HSS peer dictionary. Default: Disabled

standard-r9

Sets the Diameter dictionary to the standard HSS peer dictionary for release 9. Default: Enabled

eir-dictionary { custom1 | standard }

Specifies that an Equipment Identity Register (EIR) dictionary is to be used in conjunction with the HSS Diameter dictionary.
custom1: Sets the EIR Diameter dictionary to a customer-specific EIR Diameter dictionary.
standard: Sets the EIR Diameter dictionary to the standard HSS peer dictionary.
standard-r9: Sets the EIR Diameter dictionary to the standard HSS peer dictionary for release 9.

Usage

Use this command to select the Diameter dictionary for the HSS peer service.

Example

The following command sets the Diameter dictionary to IETF RFC 4006 specific:

```
diameter hss-dictionary standard
```

diameter hss-endpoint

Associates a preconfigured Diameter origin endpoint with this HSS peer service.

Product

MME

Privilege

Administrator

Syntax

diameter hss-endpoint *endpoint_name* **[eir-endpoint** *eir_endpoint_name* **]**

no diameter hss-endpoint

no

Removes previously associated Diameter origin endpoint from this HSS peer service.

endpoint_name

Identifies a preconfigured Diameter endpoint specific to the HSS interface. The endpoint must be present in all Diameter messages and is the endpoint that originates the diameter message.
endpoint_name is a preconfigured Diameter endpoint name expressed as an alphanumeric string of 1 through 63 characters.

eir-endpoint *eir_endpoint_name*

Identifies a preconfigured Diameter endpoint specific to the S13 Equipment Identity Register (EIR) interface.
eir_endpoint_name must be an existing Diameter endpoint expressed as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to associated a Diameter origin endpoint to create a Diameter-based S6a interface association in this HSS peer service to provide AAA functionality to the EPS bearer context.
Optionally, use this command to associate a Diameter origin endpoint to create a Diameter-based S13 interface association in this HSS peer service to provide IMEI query capability between the MME and an EIR.
Refer to the *Diameter Endpoint Configuration Mode Commands* chapter for more information on Diameter endpoint configuration parameters.

Example

The following command associates the preconfigured Diameter endpoint *hss_1* with this HSS peer service for HSS interface support.

```
diameter hss-endpoint hss_1
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

failure-handling

Configures failure handling behavior in the event of a failure with the HSS peer service. It also defines the action on various error codes on the Diameter interface during authentication or session activities.

Product

MME

Privilege

Security Administrator, Administrator

Syntax

failure-handling { authentication-information-request | check-identity-request | notify-request | purge-ue-request | update-location-request } { diameter-result-code *start_error_code* **[to** *end_error_code* **] | request-timeout } action { continue | retry-and-terminate | terminate }**

no failure-handling { authentication-information-request | check-identity-request | notify-request | purge-ue-request | update-location-request } diameter-result-code *start_error_code* **[to** *end_error_code* **]**

default failure-handling { authentication-information-request | check-identity-request | notify-request | purge-ue-request | update-location-request } request-timeout

no

Removes the preconfigured failure handling procedures for calls in an HSS peer service.

default

Sets the default action for failure handling procedure for calls in an HSS peer service.
For default actions on Diameter result/error codes see the *Usage* section below.

authentication-information-request

Configures the MME-HSS service to handle the failures in an Auth-Information-Request message.

check-identity-request

Configures the MME-HSS service to handle the failures in a Check-Identity-Information-Request message.

notify-request

Configures the MME-HSS service to handle the failures in a Notify-Request message.

purge-ue-request

Configures the MME-HSS service to handle the failures in a Purge-UE-Request message.

update-location-request

Configures the HSS peer service to handle the failures in an Update-Location-Request message.

diameter-result-code *start_error_code* **[to** *end_error_code***]**

Configures the HSS peer service to handle the failures for various request message having specific single or range of Diameter result codes in a request message.
start_error_code specifies an individual error code for Diameter protocol as an integer from 3000 through 5999. This will be the starting of code if a range of error codes is specified with the optional keyword **to** *end_error_code*.
to *end_error_code* is used to specify a range of error codes to handle by this command.
end_error_code specifies the end error code for Diameter protocol as an integer from 3000 through 5999.

request-timeout

Configures the HSS peer service to handle the failures for various request messages if response to that message is not received before timeout duration exhausted.

action { continue | retry-and-terminate | terminate }

Specifies the action to be taken on failure of any message as a policy for failure handling.

- **continue**: On receipt of any error, the system allows the HSS peer service to continue with the session procedure without any interruption.
- **retry-and-terminate**: On receipt of any error, the system instructs the HSS peer service to retry the procedure. The system will retry up to the configured number of attempts and terminate the session/procedure if it received a subsequent number of errors after retry attempts.
- **terminate**: The system allows the HSS peer service to terminate the session procedure without any retry attempt on the event of any failure.

Usage

Use this command to configure the failure handling behavior in the event of a communication failure with the HSS peer service.
The following are the default action for Diameter result codes:

- For all protocol error codes 3000 to 3999, the default action is terminate. For all transient error codes 4000, 4001, 4004 to 4180, and 4182 to 4999, the default action is continue.
- For transient error codes 4002, 4003, and 4181, the default action is retry.
- For error code 4001, the default action is terminate.
- For permanent error codes 5000 to 5999, the default action is terminate

Example

The following command will allow HSS peer service to continue if any failure in Auth-Information-Request message occurred with Diameter error code *3050*:

```
failure-handling authentication-information-request diameter-result-code
3050 action continue
```

request timeout

Configures the application request timeout between the HSS peer service and HSS node. The MME waits for this duration before retransmitting the request to corresponding HSS node.

Product

MME

Privilege

Administrator

Syntax

request timeout *dur*

[no | default] request timeout

no

Disables the configured application request timeout value.

default

Sets the application request time out duration to default value of 300 seconds.

dur

Specifies the application request timeout duration (in seconds) as an integer from 1 through 300. The MME will wait for this duration before retrying the request with corresponding HSS. Default: 300

Usage

Use this command to set the waiting period for HSS peer service in seconds after which the request is deemed to have failed or system will resend the request.

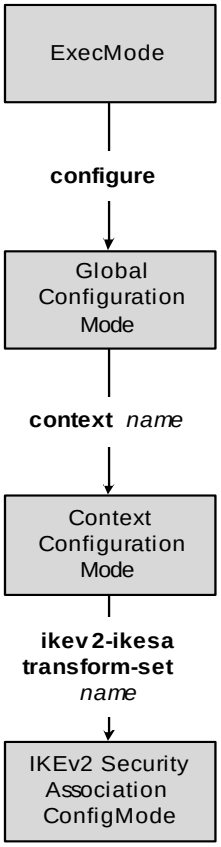
Example

The following example configures the application request timeout duration to 300 seconds:

```
default request timeout
```

Chapter 151
IKEv2 Security Association Configuration Mode Commands

The IKEv2 Security Association Configuration Mode is used to configure a Security Association (SA) at the outset of an IPSec session. A security association is the collection of algorithms and parameters (such as keys) that is being used to encrypt and authenticate a particular flow in one direction. In normal bi-directional traffic, the flows are secured by a pair of security associations.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

default

Sets the default properties for the selected parameter.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

default { encryption | group | hmac | lifetime | prf }

Set the defaults for the following parameters:

- **encryption**: Default algorithm for the IKEv2 IKE SA is AES-CBC-128.
- **group**: Default Diffie-Hellman group is Group 2.
- **hmac**: Default IKEv2 IKE SA hashing algorithm is SHA1-96.
- **lifetime**: Default lifetime for SAs derived from this transform-set is 86400 seconds.
- **prf**: Default PRF for the IKEv2 IKE SA is SHA1.

Usage

Configure default parameters for the IKEv2 IKE SA transform-set.

Example

Use the following configuration to set the default encryption algorithm:

```
default encryption
```

encryption

Configures the appropriate encryption algorithm and encryption key length for the IKEv2 IKE security association. AES-CBC-128 is the default.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

```
encryption { 3des-cbc | aes-cbc-128 | aes-cbc-256 | des-cbc }

default encryption
```

3des-cbc

Data Encryption Standard Cipher Block Chaining encryption applied to the message three times using three different cypher keys (triple DES).

aes-cbc-128

Advanced Encryption Standard Cipher Block Chaining with a key length of 128 bits.

aes-cbc-256

Advanced Encryption Standard Cipher Block Chaining with a key length of 256 bits.

des-cbc

Data Encryption Standard Cipher Block Chaining. Encryption using a 56-bit key size. Relatively insecure.

Usage

IKEv2 requires a confidentiality algorithm to be applied in order to work.
In cipher block cryptography, the plaintext is broken into blocks usually of 64 or 128 bits in length. In cipher block chaining (CBC) each encrypted block is chained into the next block of plaintext to be encrypted. A randomly-generated vector is applied to the first block of plaintext in lieu of an encrypted block. CBC provides confidentiality, but not message integrity.
Because RFC 4307 calls for interoperability between IPSec and IKEv2, the IKEv2 confidentiality algorithms must be the same as those configured for IPSec in order for there to be an acceptable match during the IKE message exchange. Because of RFC4307, in IKEv2, there is no viable NULL option, it is available for testing only.

Example

The following command configures the encryption to be the default aes-cbc-128:

```
default encryption
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

group

Configures the appropriate key exchange cryptographic strength by applying a Diffie-Hellman group. Default is Group 2.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

```
group { 1 | 2 | 5 | 14 }

default group
```

1

Configures crypto strength at the Group 1 level. Lowest security.

2

Configures crypto strength at the Group 2 (default) level. Medium security.
This is the default setting for this command.

5

Configures crypto strength at the Group 5 level. Higher security.

14

Configures crypto strength at the Group 14 level. Highest security

Usage

Diffie-Hellman groups are used to determine the length of the base prime numbers used during the key exchange process in IKEv2. The cryptographic strength of any key derived depends, in part, on the strength of the Diffie-Hellman group upon which the prime numbers are based.
Group 1 provides 768 bits of keying strength, Group 2 provides 1024 bits, Group 5 provides 1536 bits and Group 14 provides 2048 bits of encryption strength.
Configuring a DH group also enables Perfect Forward Secrecy, which is disabled by default.

Example

This command configures security at the default level (Group 2):

```
default group
```

hmac

Configures the IKEv2 IKE SA integrity algorithm. Default is SHA1-96.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

```
hmac { md5-96 | sha1-96 | sha2-256-128 | sha2-384-192 | sha2-512-256 }

default hmac
```

md5-96

HMAC-MD5 uses a 128-bit secret key and produces a 128-bit authenticator value.

sha1-96

HMAC-SHA-1 uses a 160-bit secret key and produces a 160-bit authenticator value. This is the default setting for this command.

sha2-256-128

HMAC-SHA-256 uses a 256-bit secret key and produces a 128-bit authenticator value.

sha2-384-192

HMAC-SHA-384 uses a 384-bit secret key and produces a 192-bit authenticator value.

sha2-512-256

HMAC-SHA-512 uses a 512-bit secret key and produces a 256-bit authenticator value.

Usage

IKEv2 requires an integrity algorithm be configured in order to work.
A keyed-Hash Message Authentication Code, or HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key to verify both data integrity and message authenticity. A hash takes a message of any size and transforms it into a message of a fixed size: the authenticator value. This is truncated and transmitted. The authenticator value is reconstituted by the receiver and the first truncated bits are compared for a 100 percent match.
Because RFC 4306 calls for interoperability between IPSec and IKEv2, the IKEv2 integrity algorithms must be the same as those configured for IPSec in order for there to be an acceptable match during the IKE message exchange.

Example

The following command configures the default HMAC value (SHA1-96):

```
default hmac
```

lifetime

Configures the lifetime of a security association (SA) in seconds.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

lifetime *sec*

default lifetime

lifetime *sec*

Sets the value of the timeout parameter in seconds as an integer from 60 through 86400. Default: 86400

Usage

The secret keys that are used for various aspects of a configuration should only be used for a limited amount of time before timing out. This exposes a limited amount of data to the possibility of hacking. If the SA expires, the options are then to either close the SA and open an new one, or renew the existing SA.

Example

The following command sets the lifetime timeout to be the default value (86400):

```
default lifetime
```

prf

Selects one of the HMAC integrity algorithms to act as the IKE Pseudo-Random Function. A PRF produces a string of bits that an attacker cannot distinguish from random bit string without knowledge of the secret key. The default is SHA1.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

```
prf { md5 | sha1 | sha2-256 | sha2-384 | sha2-512 }

default prf
```

md5

MD5 uses a 128-bit secret key and produces a 128-bit authenticator value.

sha1

SHA-1 uses a 160-bit secret key and produces a 160-bit authenticator value.
SHA-1 is considered cryptographically stronger than MD5, but it takes more CPU cycles to compute.
This is the default setting for this command.

sha2-256

PRF-HMAC-SHA-256 uses a 256-bit secret key.

sha2-384

PRF-HMAC-SHA-384 uses a 384-bit secret key.

sha2-512

PRF-HMAC-SHA-512 uses a 512-bit secret key.

Usage

This command generates keying material for all the cryptographic algorithms used in both the IKE_SA and the CHILD_SAs.

Example

This configuration sets the PRF to be the default value (sha1):

```
default prf
```

Chapter 152
IMEI Profile Configuration Mode

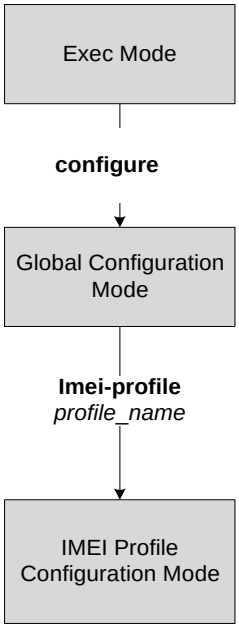
The IMEI profile configuration mode defines a set of parameters controlling the SGSN behavior when a Request is received from a device in the specified IMEI (International Mobile Equipment Identity) range. An IMEI profile is a key element in the Operator Policy feature and an IMEI profile is not used or valid unless it is associated with an IMEI range and this association is specified in an operator policy (see the *Operator Policy Configuration Mode Commands* chapter elsewhere in the *Command Line Interface Reference*).

Essentially, an IMEI profile is a template which groups a set of device-specific commands that may be applicable to one or more IMEIs. The same IMEI profile can be associated with multiple IMEI ranges and multiple operator policies.

An SGSN supports a total of 1000 IMEI profile configurations.

When this mode is accessed, the command prompt should resemble:

```
[local]asr5000(imei-profile-<profile_name>)#
```



associate

Associate an APN remap table with this IMEI profile.

Note that an APN remap table can be associated with an IMEI profile before the table has actually been created/configured.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

associate apn-remap-table *table_name*

no associate apn-remap-table

no

Disables the configured remap table association.

table_name

Define the name of an APN remap table that is to be associated with this IMEI profile for call routing based in IMEI.

Usage

Use this command to associate an APN remap table with this IMEI profile. With such an association, it is possible to override an APN call-routing based on an IMEI.
For example, with the APN exceptions defined in an APN remap table (refer to the *APN Remap Table Configuration Mode* chapter), a blank APN or an incorrect APN could be overriden. So during PDP Activation for in incoming call, the call could be rerouted based on an IMEI in the range defined for the IMEI profile.

Example

Associate the APN remap table ‘remapHO’ (remaps all calls with blank APNS to the head-office) to this IMEI profile:

```
associate apn-remap-table remapHO
```

blacklist

Blacklist all mobile devices that fit the IMEI definitions associated with this IMEI profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

blacklist

remove blacklist

remove

Including this keyword with the command, removes the blacklist command from the IMEI profile configuration.

Usage

Blacklists subscribers whose devices bear IMEI that match the defined IMEI range for this profile.

Example

Use this command to black list all subscribers with IMEI that fall within the range set for this IMEI profile:

blacklist

description

Define a descriptive string relevant to the specific APN profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

description *description*

remove description

remove

Removes the configured description from this APN profile.

description

Enter an alphanumeric string of 1 to 100 alphanumeric characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotes (“).

Usage

Define information that identifies this particularly APN profile.

Example

Indicate that this IMEI profile *IMEIprof1* is to be used for customers in the United Kingdom and that the profile:

```
description “IMEIprof1 defines routing actions based on IMEI for
customers in the UK.”
```

direct-tunnel

Instruct the SGSN to enable/disable a direct tunnel between the RNC and the GGSN based on the IuPS service configuration.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
direct-tunnel check-iups-service

no direct-tunnel
```

no direct-tunnel

This command instructs the SGSN to disable the direct tunnel function between the GGSN and the RNC.

Usage

Direct tunnel is enabled by default on the GGSN and often on the RNC. This leaves it to the SGSN's configuration to actually enable or disable a direct tunnel.
With the SGSN, the options for configuring a direct tunnel are complex -- enable/disable on the basis of APNs, or RNCs, or GGSNs, or on the basis of the IMEI range. Refer to the *SGSN Administration Guide* for configuration details.

Example

Assuming the IuPS service configuration has enabled DT for associated RNCs, then use this command to enable DT from the RNC to the GGSN associated with this IMEI profile:

```
direct tunnel check-iups-service
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Return to the Exec mode.

exit

Exits the current configuration mode and returns to the context configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Move to the previous configuration mode.

ggsn-address

Identify the target GGSN for traffic being managed by this IMEI profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ggsn-address *IPv4/IPv6_address*

IPv4/IPv6_address

Enter the IP address of the target GGSN. Enter the address in either standard IPv4 dotted decimal format or in standard IPv6 colon notation format.

Usage

Use this command to define the IP address of the target GGSN to be associated with this IMEI profile.

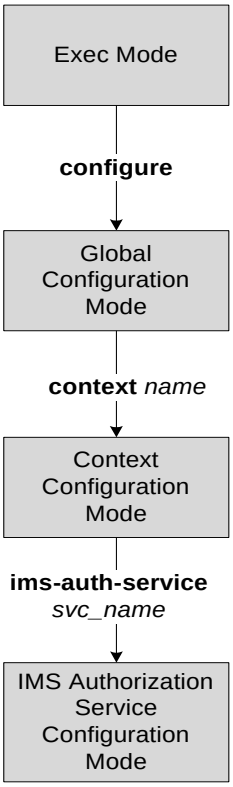
Example

The following command identifes the address of the GGSN associated with this IMEI profile as 123.123.11.1

ggsn-address *123.123.11.1*

Chapter 153
IMS Authorization Service Configuration Mode Commands

The IMS Authorization Service Configuration Mode enables to configure IP Multimedia Subsystem (IMS) authorization services to manage policy control functions and Gx interface support.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

p-cscf discovery

This command defines the method of Proxy-Call Session Control Function (P-CSCF) discovery to be used.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
p-cscf discovery { table { 1 | 2 } [ algorithm { ip-address-modulus | msisdn-modulus |
round-robin } ] | diameter-configured }

[ default | no ] p-cscf discovery
```

default

Sets the P-CSCF discovery to default parameter.

no

Removes/deletes configured parameters for P-CSCF discovery.

table { 1 | 2 }

Specifies that which P-CSCF table is to be used to obtain the primary and secondary P-CSCF addresses. Total 2 tables can be configured for P-CSCF discovery.

algorithm { ip-address-modulus | msisdn-modulus | round-robin }

Specifies the algorithm to select the row from the P-CSCF table to be used for P-CSCF discovery.

- **ip-address-modulus**: This algorithm divides the IP address, in binary, of the subscriber by the number of rows in the table, and the remainder is used as an index into the specified table to select the row.
- **msisdn-modulus**: This algorithm divides the MSISDN value, in binary without the leading "+", of the subscriber by the number of rows in the table, and the remainder is used as an index in the specific table to select the row.
- **round-robin**: This algorithm rotates all rows in the active table for selection of the row in round-robin way. If no algorithm is specified this is the default behavior.

Default: **round-robin**

diameter-configured

This option enables the table number and algorithm specified by the **diameter host-select table** configuration in Policy Control Configuration mode.
If the primary host in that configuration is down it assumes that the primary P-CSCF in the row of P-CSCF table is also down, and it does not return that IP address in the create PDP context response.
This option also performs the deactivation processing of the PDP contexts when Diameter Policy Control Application (DPCA) switches, host tables as detailed in the **diameter host-select** command description in Policy Control Configuration mode.

Usage

Use this command to configure the table and row selection methods to select IP address/host address for P-CSCF discovery.

Example

The following command specifies **table 1** with **round-robin** algorithm to select the rows with IP address for P-CSCF discovery.

```
p-cscf discovery table 1 algorithm round-robin
```

p-cscf table

This command adds/appends rows with primary and/or secondary IPv4/IPv6 addresses to a P-CSCF discovery table with precedence for P-CSCF discovery.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
p-cscf table { 1 | 2 } row-precedence precedence_value { address ip_address | ipv6-
address ipv6_address } [ secondary { address ip_address | ipv6-address ipv6_address } ]

no p-cscf table { 1 | 2 } row-precedence precedence_value
```

no

Removes/deletes configured row with precedence in specified table for P-CSCF discovery address.

{ 1 | 2 }

Specifies which P-CSCF table is to be used to add/append the primary and secondary P-CSCF addresses. Two tables can be configured for P-CSCF discovery address.

row-precedence *precedence_value*

This keyword adds/appends the row with the specified row-precedence to the P-CSCF address table.
In 8.1 and later releases, *precedence_value* must be an integer from 1 through 128, and a maximum of 128 rows can be added to a table.
In release 8.0, *precedence_value* must be an integer from 1 through 100, and a maximum of 16 rows can be added to a table.

secondary

Specifies the secondary IPv4/IPv6 address to be entered in P-CSCF table rows.

address *ip_address*

Specifies the primary and/or secondary IPv4 address for P-CSCF discovery table. This keyword, if used with **secondary** keyword, specifies the secondary IPv4 address.
ip_address must be entered in IPv4 dotted-decimal notation.

ipv6-address *ipv6_address*

Specifies the primary and/or secondary IPv6 address for P-CSCF discovery table. This keyword, if used with **secondary** keyword, specifies the secondary IPv6 address.
ipv6_address must be entered in IPv6 colon-separated notation.

Usage

Use this command to add rows with primary and/or secondary IP addresses for P-CSCF discovery. The row is added with the specified row-precedence.

The operator can add/remove rows to the table that is not currently selected by the **diameter host-select table** command in Policy Control Configuration Mode.

Example

The following command adds a row in **table 2** with primary IP address *10.2.3.4*, secondary IP address as *50.6.7.8*, and row-precedence value as *20* for P-CSCF discovery.

```
p-cscf table 2 row-precedence 20 address 10.2.3.4 secondary 50.6.7.8
```

policy-control

This command enters the Policy Control Configuration mode for Diameter Policy Control Application (DPCA) to configure Diameter authorization and policy control parameter for IMS authorization.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] policy-control
```

no

Disables the pre-configured policy control parameters for IMS authorization in this IMS authorization service.

Usage

Use this command to enter the Policy Control Configuration Mode to configure the policy control parameters for Diameter authorization and charging policy in IMS Authorization Service.
Entering this command results in the following prompt:
`[context_name]hostname(config-imsa-dpca)#`
Policy Control configuration commands are described in the *Policy Control Configuration Mode Commands* chapter.

qos-update-timeout

This command is obsolete in release 11.0 and later releases. This command sets the Quality of Service update timeout for a subscriber in IMS authorization service.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

qos-update-timeout *timeout_duration*

no qos-update-timeout

no

Disables the pre-configured QoS update timeout parameter in this IMS authorization service.

timeout_duration

Specifies the duration of timeout in seconds as an integer from 0 through 3600.
Default: 60

Usage

Use this command to set the maximum time to wait for a subscriber to initiate the update QoS procedure in IMS authorization service.

Example

The following command sets the QoS update timeout to *90* seconds.

```
qos-update-timeout 90
```

signaling-flag

This command specifies whether a request for a PDP context dedicated to signaling (for IMS sessions) should be granted or denied.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
signaling-flag { deny | permit }

default signaling-flag
```

default

Sets the signaling flag to default mode of deny.

deny

Denies the request for a signaling PDP context for IMS session and keeps signaling co-existed with other traffic on PDP contexts. Default: Enabled

permit

Permits the request for a signaling PDP context for IMS session and a separate signaling context activated. Default: Disabled

Usage

Use this command to allow or deny the activation of a dedicated PDP context for signaling. The user equipment (UE) may indicate that the PDP context should be dedicated for IP multimedia (IM) signaling by setting the IP Multimedia Core Network (IM-CN) signaling flag in the Protocol Configuration Options (PCO).
The **deny** option causes the system to inform the UE that the PDP context will not be dedicated for IM signaling and signaling will co-exist with other traffic on PDP context.
The **permit** option is used to activate the signaling context for signal traffic and the other traffic uses other PDP context for traffic with the following destinations:

- Towards the DHCP and DNS servers for the IMS domain
- Towards the P-CSCF(s)

The UE is not trusted to follow these restrictions, and the system monitors and restricts the traffic from the dedicated PDP context. The **signaling-flow class-map** command is used to configure the restrictions.

Example

The following command denies the request for a signaling PDP context for IMS session.

```
default signaling-flag
```

signaling-flow

This command specifies the packet filters and policy servers for bandwidth control and singling context enforcement that define the traffic that is allowed through the dedicated signaling context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

signaling-flow permit server-address *ipv4/ipv6_address* **[server-port {** *port_num* **| range** *start_port* **to** *end_port* **}] [description** *STRING* **]**

no signaling-flow permit server-address *ipv4/ipv6_address* **[server-port {** *port_num* **| range** *start_port* **to** *end_port* **}]**

no

Disables the signaling flow option configured with this command.

server-address *ipv4/ipv6_address*

The server address refers to the destination IP address in uplink packets, and the source IP address in downlink packets.
ipv4/ipv6_address is an IP address in IPv4 dotted-decimal or IPv6 colon-separated notation and can be used with a subnet mask.
A maximum of 16 signaling server addresses can be configured per IMS Authorization service.

server-port { *port_num* **| range** *start_port* **to** *end_port* **}**

Specifies the TCP/UDP port number(s) of the server to be used for communication.
port_num must be an integer from 1 through 65535.
range *start_port* **to** *end_port* provides the option to configure the range of ports on server for communication.
start_port must be an integer from 1 through 65535 but lesser than *end_port*, and *end_port* must be an integer from 1 through 65535 but greater than *start_port*.

description *STRING*

Specifies the customized description for configured signaling server as an alphanumeric string of 1 through 63 characters.

Usage

Traffic that matches any instance of the signaling-flow command will be forwarded via the signaling PDP context. In addition, the policy server gives policy gates to use for the signaling PDP context.

Example

The following command sets the packet filter server address to *10.2.3.4* with port number *1234* for packet filtering.

```
signaling-flow server-address 10.2.3.4 server-port 1234
```

traffic-policy

This command specifies the action on packets which do not match any policy gates in the general purpose PDP context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink } {
forward | discard }

default traffic-policy general-pdp-context no-matching-gates direction { downlink |
uplink }
```

default

Sets the default traffic policy for packets without any policy gate match in general purpose PDP context. By default packets which do not have any matching policy gate are forwarded.

no-matching gates

Applies traffic policy for packets which do not match any policy gate.

direction { downlink | uplink }

Specifies the direction of traffic to apply this traffic policy in general PDP context.
downlink: Specifies the traffic from system to MN. Default is set to forward.
uplink: Specifies the traffic from MN to system. Default is set to forward.

forward

Forwards the packets which do not match any policy gates. Default: Enabled

discard

Discards the packets which do not match any policy gates. Default: Disabled

Usage

This command provides configuration on traffic policy applied on packets which are not matching any policy gate in general PDP context. Packets can either be forwarded or discarded on the basis of operator's configuration.
This command needs to be configured once for downlink and once for uplink separately.

Example

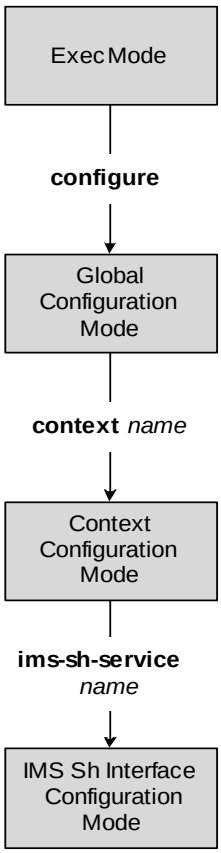
The following command discards uplink packets which do not match any policy gate in general purpose PDP context.

```
traffic-policy general-pdp-context no-matching-gates direction uplink
discard
```

Chapter 154
IMS Sh Service Configuration Mode Commands

The IMS Sh Interface Configuration Mode is used to configure various Diameter parameters in order for:

PDIF to communicate with the HSS server. HSS server is used for MAC address validation in the IKEv2 exchanges to set up SAs and for storing part of the user profile.SCM to communicate with the HSS server. HSS server is used for retrieval and update of call feature parameters and call restriction data.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

diameter

This command configures Diameter parameters.

Product

PDIF, SCM

Privilege

Administrator

Syntax

```
diameter { dictionary { custom1 | standard | endpoint string }
default diameter { dictionary | endpoint }
no diameter endpoint
```

no

Removes previously configured endpoint.

default

Configures parameters to the default value.

dictionary

Specifies the dictionary to use.

- **custom1**: A custom dictionary
- **standard**: The standard dictionary

Important: SCM uses only the standard dictionary.

endpoint *string*

Selects an endpoint to use in the configuration.
string must be the endpoint name, and must be an alpha and/or numeric string of 1 through 63 characters in length.

Usage

The Diameter endpoint contains information on the peer names and IP addresses and port, and the local IP address to use for Diameter.
You can have more than one Diameter endpoint configured on the chassis and the ims-sh-service needs to know which Diameter endpoint to use. This command is to select the appropriate Diameter endpoint, even if only one has been configured.

Example

The following example selects a diameter endpoint *diam1:*

```
diameter endpoint diam1
```

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to change to the Exec Mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

failure-handling

This command configures the action to take in the event of an HSS server request failure.

Product

PDIF, SCM

Privilege

Administrator

Syntax

[default] failure-handling { profile-update-request | user-data-request } { { diameter-result-code *result_code* **[to** *result_code* **] } | timeout } action { continue | retry-and-terminate | terminate } } }**

---

default

Resets configuration for the specified keyword to the default setting.

---

profile-update-request

Configures failure-handling as a result of a profile update request error.

---

user-data-request

Configures failure-handling as a result of a user data request.

---

diameter-result-code *result_code* **[to** *result_code* **]**

The Result-Code data field contains a space representing errors. Diameter provides the following classes of errors, all identified by the thousands digit in the decimal notation:

- 3xxx (Protocol Errors)
- 4xxx (Transient Failures)
- 5xxx (Permanent Failure)

result_code specifies either a result code value (**diameter-result-code** *3001*) or a range of result code values (**diameter-result-code** *3000* **to** *9999*) to which the failure-handling applies.

---

action

Configures the action to take depending on the diameter-result-code:

- Continue the session
- Retry and then terminate
- Terminate the session

---

request-timeout action

Configures the action to take as a result of a request timeout error:

- Continue the session
- Retry and then terminate
- Terminate the session

Usage

Configures all failure-handling parameters.

Example

The following command configures profile-update-request failure-handling using a result-code configuration with the terminate session option:

```
failure-handling profile-update-request diameter-result-code 3005 to
3600action terminate
```

request

Configures application request timeout.

Product

PDIF, SCM

Privilege

Administrator

Syntax

request timeout *secs*

[no | default] request timeout

no

Disables a configured timeout request.

default

Default: 300 seconds
Resets configuration to the default setting.

request timeout *secs*

Configures the request timeout in seconds.
secs must be an integer from 1 through 300.

Usage

Specifies the session request timeout period in seconds after which the request is deemed to have failed.

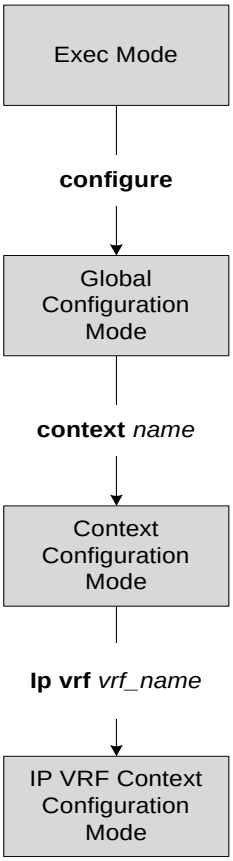
Example

The following example configures the default timeout request of 300 seconds:

```
default request timeout
```

Chapter 155
IP VRF Context Configuration Mode Commands

The IP VRF Context Configuration Mode is used to create and manage the Virtual Routing and Forwarding (VRF) context instance for BGP/MPLS VPN, GRE, IPSec tunneling or service interfaces for virtual routing, addresses, address resolution options, etc.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

ip maximum-routes

This command configures the maximum number of routes in an IP VRF routing table configured in this context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip maximum-routes *max_routes*

no ip maximum-routes

no

Disables the configured maximum routes in specific IP VRF context.

max_routes

Sets the maximum number of routes in a specific IP VRF context.
max_routes must be an integer from 1 through 16384.

Usage

Use this command to configure the maximum number of routes in a particular VRF routing table. When the number of routes in the VRF is more than the maximum limit configured, a critical log is generated indicating that the number of routes is over the limit. Once the number of routes in the VRF goes under the limit, a **clear log** is generated.
The maximum routes configured using this command will be sent to the threshold configuration logic for appropriate action. For more information on threshold configuration, refer to descriptions of the **threshold route-service bgp-routes** and **threshold poll route-service interval** commands in the *Global Configuration Mode Commands* chapter.

Example

The following command sets *1000* routes as a maximum limit for specific VRF context:

```
ip maximum-routes 1000
```

mpls map-dscp-to-exp

This command maps the final differentiated services code point (DSCP) bit value in the IP packet header to the final Experimental (EXP) bit value in the MPLS header for incoming traffic.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] mpls map-dscp-to-exp dscp dscp_bit_value exp exp_bit_value
```

no

Disables the configured DSCP bit value mapping to the EXP bit value from a specific IP VRF context.

dscp *dscp_bit_value*

Specifies the final DSCP bit value which is to map with the final EXP bit value in MPLS header for incoming traffic.
dscp_bit_value specifies the value of DSCP bit values separated in eight groups and represented with integers from 0 through 7.
The default representation of DSCP value in eight groups is given in the following table:

DSCP Marking Value	DSCP Map Group
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

exp *exp_bit_value*

Specifies the final EXP bit value in MPLS header to which the final DSCP bit value 0 to 7 (represented in eight values) coming from incoming traffic will be mapped.
exp_bit_value is the value of EXP bit in MPLS header and must be an integer between 0 through 7.

Usage

Use this command to map the final DSCP value coming from incoming IP traffic to a final EXP value in MPLS header. This mapping determines the QoS and service parameters to which the packet is assigned.

Example

The following command maps the DSCP value *3* (24 to 31) to EXP bit *3* in MPLS header:

```
mpls map-dscp-to-exp dscp 3 exp 3
```

mpls map-exp-to-dscp

Maps incoming the Experimental (EXP) bit value in MPLS header to the internal differentiated services code point (DSCP) bit value in IP packet headers for outgoing traffic.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] mpls map-exp-to-dscp exp exp_bit_value dscp dscp_bit_value
```

no

Disables the configured EXP bit value mapping to DSCP bit value from specific IP VRF context.

exp *exp_bit_value*

Specifies the incoming EXP bit value in MPLS header to which the internal DSCP bit value 0 to 7 (represented in 8 values) in IP traffic will be mapped.
exp_bit_value is the value of the EXP bit in an MPLS header and must be an integer from 0 through 7.

dscp *dscp_bit_value*

Maps the DSCP bit value with the incoming EXP bit value in an MPLS header.
dscp_bit_value specifies the value of the DSCP bit values separated in eight groups and represented with integers between 0 through 7.
The default representation of DSCP value in eight groups is given in the following table:

DSCP Marking Value	DSCP Map Group
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Usage

Use this command to map the incoming EXP bit value in MPLS headers to the DSCP bit value in IP traffic. This mapping determines the QoS and service parameters to which the packet is assigned.

Example

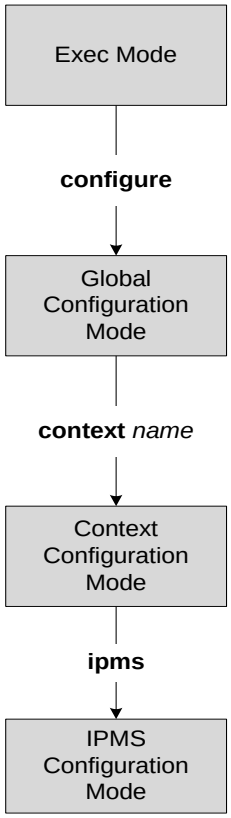
The following command maps the EXP bit value *4* to DSCP value *6* (48 to 55) in IP header:

```
mpls ap-exp-to-dscp exp 4 dscp 6
```

Chapter 156
IPMS Client Configuration Mode Commands

The IPMS Client Configuration Mode is used to enable the Intelligent Packet Monitoring System (IPMS) client service on an Access Gateway and to set basic service-wide options in a context.

Important: This is a license enabled external application support. For more information on this product, refer to the *IPMS Installation and Administration Guide*.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

export keys

Enables the encryption key export in specific key exchange events to IPMS server from IPMS-enabled AGW.

Important: This is a license enabled customer specific command.

Product

IPMS

Privilege

Security Administrator, Administrator

Syntax

no

Removes the configured source IP address from this context for IPMS client communication with IPMS server.

ikev2

Enables the security association (SA) key export for Internet Key Exchange (IKEv2) protocol to IPMS server.

Usage

Monitor subscribers which have complaints of service availability or to monitor a test user for system verification.

Example

The following command assigns the IP address *10.2.3.4* to the IPMS client service in context to communicate with IPMS server. This is the IP address allocated for IPMS client service on chassis.

```
source address 10.2.3.4
```

heartbeat

Configures the IPMS heartbeating between the IPMS-enabled AGW and the IPMS server.

Product

IPMS

Privilege

Security Administrator, Administrator

Syntax

heartbeat period *dur* [**permitted-failure***no_of_failures*]

[**no** | **default**] **heartbeat**

default

Configures the heartbeat period and permitted number of failures to the default values of 10 seconds and 1 failure respectively.

no

Disables/removes the configured heartbeat period and permitted number of failures.

period *dur*

Specifies the periodicity (in seconds) between heartbeat messages as an integer from 1 through 3600. Default: 10

permitted-failure *no_of_failures*

Specifies the number of errors/failures allowed before declaring an IPMS server as dead/unreachable as an integer from 1 through 10. Default: 1

Usage

Use this command to configure the heartbeat message periodicity and permissible failure of heartbeat message response before declaring an IPMS server as dead or unreachable. When an IPMS server is declared down an SNMP trap is sent.

Example

Following command configures the heartbeat message periodicity to *5* second and number of failures allowed as *3* to determine an IPMS server as dead.

```
heartbeat period 5 permitted-failure 3
```

server

Configures the IPMS server address and ports on which the IPMS client on an IPMS-enabled AGW communicates. This is the IP address and port range of the IPMS server.

Product

IPMS

Privilege

Security Administrator, Administrator

Syntax

server address*ip_address* [**seconary**] [**start-port** *start_port* [**end-port** *end_port*]][**secondary**]

no server address *ip_address*

no

Removes the configured IPMS server IP address and port range from this context.

address *ip_address*

Specifies the IP address of the IPMS server to which the IPMS client service communicates in IPv4 dotted-decimal notation.
A maximum of 4 IPMS severs can be configured with this command in one context.

[start-port *start_port***[end-port** *end_port* **]]**

Default: 45001 source port
45005 end port
Specifies the range of UDP ports on which IPMS client communicates with the IPMS server.
start-port *start_port*: Specifies starting port number as an integer from 1 through 65535 that is less than *end_port*, if end-port is specified.
end-port *end_port*: Specifies is the end port number as an integer from 1 through 65535 that is more than *start_port*.

secondary

The secondary keyword is used to configure the specified server address as secondary IP address on the IPMS client interface.

Usage

Use this command to configure/remove the IPMS servers. Up to 4 different IPMS servers can be configured with this command. UDP port number can also be configured with this command. IPMS client will search for this IP address to push the event and traffic logs.

Example

The following command configures IPMS server having IP address *10.2.3.4* in the IPMS client service export the event and traffic logs for intelligent packet monitoring functionality. It also specifies the UDP port range from *48000* to *48005* for communication.

```
server address 10.2.3.4 start-port 48000 end-port 48005
```

source

Configures the source address of the IPMS client in this context to communicate with the IPMS server. This is the IP address for IPMS client on the chassis.

Product

IPMS

Privilege

Security Administrator, Administrator

Syntax

source address*ip_address*

address *ip_address*

Specifies the IP address of the IPMS client on the AGW in this context. This is the address which is bound to the IPMS client service in this context.
ip_address is expressed in IPv4 dotted-decimal notation.

Usage

Monitor subscribers which have complaints of service availability or to monitor a test user for system verification.

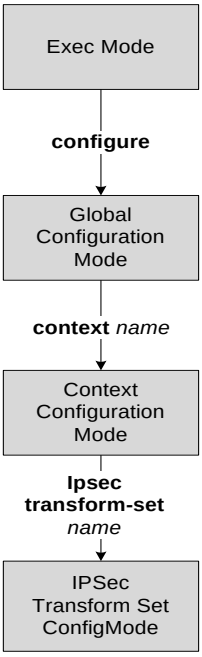
Example

The following command assigns the IP address *10.2.3.4* to the IPMS client service in context to communicate with IPMS server. This is the IP address allocated for IPMS client service on chassis.

```
source address 10.2.3.4
```

Chapter 157
IPSec Transform Set Configuration Mode Commands

The IPSec Transform Set Configuration Mode is used to configure IPSec security parameters. There are two core protocols, the Authentication Header (AH) and Encapsulating Security Payload (ESP). AH may be considered redundant as ESP can provide the same authentication services that AH does.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

encryption

Configures the appropriate IPSec ESP encryption algorithm and encryption key length. AES-CBC-128 is the default.

Product

PDIF, SCM

Privilege

Security Administrator, Administrator

Syntax

```
encryption { 3des-cbc | aes-cbc-128 | aes-cbc-256 | des-cbc | null }

default encryption
```

3des-cbc

Data Encryption Standard Cipher Block Chaining encryption applied to the message three times using three different cypher keys (triple DES).

aes-cbc-128

Advanced Encryption Standard Cipher Block Chaining with a key length of 128 bits. This is the default setting for this command.

aes-cbc-256

Advanced Encryption Standard Cipher Block Chaining with a key length of 256 bits.

des-cbc

Data Encryption Standard Cipher Block Chaining. Encryption using a 56-bit key size. Relatively insecure.

null

The NULL encryption algorithm represents the optional use of applying encryption within ESP. ESP can then be used to provide authentication and integrity without confidentiality.

default

Sets the default IPSec ESP algorithm to AES-CBC-128.

Usage

In cipher block cryptography, the plaintext is broken into blocks usually of 64 or 128 bits in length. In cipher block chaining (CBC) each encrypted block is chained into the next block of plaintext to be encrypted. A randomly generated vector is applied to the first block of plaintext in lieu of an encrypted block. CBC provides confidentiality, but not message integrity.
Because RFC 4307 calls for interoperability between IPSec and IKEv2, the IKEv2 confidentiality algorithms must be the same as those configured for IPSec in order for there to be an acceptable match during the IKE message exchange. In IKEv2, there is no NULL option.

Example

The following command configures the encryption to be the default aes-cbc-128:

```
default encryption
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

group

Configures the appropriate key exchange cryptographic strength and activate Perfect Forward Secrecy by applying a Diffie-Hellman group.

Product

PDIF, SCM

Privilege

Security Administrator, Administrator

Syntax

```
group { 1 | 2 | 5 | 14 | none }

default group
```

default group

Configures the default crypto strength to be **none** and disables Perfect Forward Secrecy.

1

Configures crypto strength at the Group 1 level. Lowest security.

2

Configures crypto strength at the Group 2 level. Medium security.

5

Configures crypto strength at the Group 5 level. Higher security.

14

Configures crypto strength at the Group 14 level. Highest security.

none

Applies no group and disables Perfect Forward Secrecy. This is the default.

default

Sets the default Diffie-Hellman group algorithm to none. This also deactivates PFS.

Usage

Diffie-Hellman groups are used to determine the length of the base prime numbers used during the key exchange process. The cryptographic strength of any key derived depends, in part, on the strength of the Diffie-Hellman group upon which the prime numbers are based.
Group 1 provides 768 bits of keying strength, Group 2 provides 1024 bits, Group 5 provides 1536 bits and Group14 2048 bits. Selecting a group automatically activates Perfect Forward Secrecy. The default value is none, which disables PFS

Example

This command configures security at Group 2 and activates PFS:

```
group 2
```

hmac

Configures the IPSec ESP integrity algorithm using a Hash-based Message Authentication Code (HMAC).

Product

PDIF, SCM

Privilege

Security Administrator, Administrator

Syntax

```
hmac { md5-96 | sha1-96 | null }

default hmac
```

md5-96

MD5-96 uses a 128-bit secret key and produces a 128-bit authenticator value.

sha1-96

SHA-1 uses a 160-bit secret key and produces a 160-bit authenticator value.
This is the default setting for this command.

null

Configures the hmac value to be null. The NULL encryption algorithm represents the optional use of applying encryption within ESP. ESP can then be used to provide authentication and integrity without confidentiality.

default hmac

Sets the default IPSec hashing algorithm to SHA1-96.

Usage

HMAC is an encryption technique used by IPSec to make sure that a message has not been altered.
A keyed-Hash-based Message Authentication Code (HMAC), is a type of message authentication code that is calculated using a cryptographic hash function in combination with a secret key to verify both data integrity and message authenticity. A hash takes a message of any size and transforms it into a message of a fixed size: the authenticator value. This is truncated to 96 bits and transmitted. The authenticator value is reconstituted by the receiver and the first 96 bits are compared for a 100 percent match.
Because RFC 4306 calls for interoperability between IPSec and IKEv2, the IKEv2 integrity algorithms must be the same as those configured for IPSec in order for there to be an acceptable match during the IKE message exchange.

Example

The following command configures the default HMAC value (SHA1-96):

```
default hmac
```

mode

Configures the security of IP datagrams based on header placement. Tunnel mode applies security to a completely encapsulated IP datagram, while Transport does not. Default is Tunnel mode.

Product

PDIF, SCM

Privilege

Security Administrator, Administrator

Syntax

```
mode { transport | tunnel }

default mode
```

transport

In Transport mode, the IPSec header is applied only over the IP payload, not over the IP header in front of it. The AH and/or ESP headers appear between the original IP header and the IP payload, as follows:
Original IP header, IPSec headers (AH and/or ESP), IP payload (including transport header).
Transport mode is used for host-to-host communications and is generally unsuited to PDIF traffic.

tunnel

In Tunnel mode, the original IP header is left intact, so a complete IP datagram is encapsulated, forming a virtual tunnel between IPSec-capable devices. The IP datagram is passed to IPSec, where a new IP header is created ahead of the AH and/or ESP IPSec headers, as follows:
New IP header, IPSec headers (AH and/or ESP), old IP header, IP payload.
Tunnel mode is used for network-to-network communications (secure tunnels between routers) or host-to-network and host-to-host communications over the Internet.
This is the default setting for this command.

default mode

Sets the default IPSec Mode to Tunnel.

Usage

IPSec modes are closely related to the function of the two core protocols, the Authentication Header (AH) and Encapsulating Security Payload (ESP). Both of these protocols provide protection by adding to a datagram a header (and possibly other fields) containing security information. The choice of mode does not affect the method by which each generates its header, but rather, changes what specific parts of the IP datagram are protected and how the headers are arranged to accomplish this.

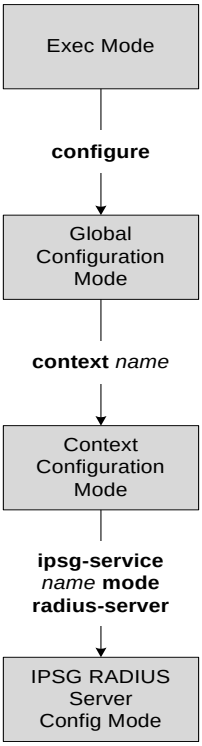
Example

The following command configures the default Tunnel mode:

```
default mode
```

Chapter 158
IPSG RADIUS Server Configuration Mode Commands

The IP Services Gateway (IPSG) RADIUS Server Configuration Mode is used to create and configure IPSG services in the current system context. The IPSG RADIUS Server Mode configures the system to receive RADIUS accounting requests as if it is a RADIUS Accounting Server, and reply after accessing those requests for user information.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

bind

Binds the IPSG RADIUS Server service to a logical AAA interface and specifies the number of allowed subscriber sessions.

Product

IPSG

Privilege

Security Administrator, Administrator

Syntax

bind { accounting-proxy address *ipv4/ipv6_address* **| address** *ipv4/ipv6_address* **} [max-subscribers** *max_sessions* **| port** *port_number* **| source-context** *source_context* **]**

bind authentication-proxy address *ipv4/ipv6_address* **[acct-port** *port_number* **| auth-port** *port_number* **| max-subscribers** *max-sessions* **| source-context** *source_context* **]**

no bind

---

no

Removes the binding for the service.

---

accounting-proxy address *ipv4/ipv6_address* **| address** *ipv4/ipv6_address* **} [max-subscribers** *max_sessions* **| port** *port_number* **| source-context** *source_context* **]**

- **accounting-proxy address** *ipv4/ipv6_address*: Specifies the IP address of the interface where accounting proxy requests are received by this service in IPv4 dotted-decimal or IPv6 colon-separated notation.
- **address** *ipv4/ipv6_address*: Specifies the IP address of the interface where accounting requests are received by this service in IPv4 dotted-decimal or IPv6 colon-separated notation.
- **max-subscribers** *max_sessions*: Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.

  In 8.3 and earlier releases, *max_sessions* must be an integer from 0 through 3000000.

  In 9.0 and later releases, *max_sessions* must be an integer from 0 through 4000000.
- **port** *port_number*: Specifies the port number of the interface where accounting requests are received by this service.

  port_number must be an integer from 1 through 65535.

  Default: 1813
- **source-context** *source_context*: Specifies the source context where RADIUS accounting requests are received.

  source_context must be an alphanumeric string of 1 through 79 characters.

  This keyword should be configured if the source of the RADIUS requests is in a different context than the IPSG service. If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

authentication-proxy address *ipv4/ipv6_address* **[acct-port** *port_number* **| auth-port** *port_number* **| max-subscribers** *max_sessions* **| source-context** *source_context* **]**

- **authentication-proxy address** *ipv4/ipv6_address*: Specifies the IP address of the interface where authentication proxy requests are received by this service in IPv4 dotted-decimal or IPv6 colon-separated notation.

  Important: Enabling authentication proxy also enables accounting proxy.

- **acct-port** *port_number*: Specifies the port number of the interface where accounting proxy requests are received by this service.

  port_number must be an integer from 0 through 65535.

  Default: 1813

- **auth-port** *port_number*: Specifies the port number of the interface where authentication proxy requests are received by this service.

  port_number must be an integer from 0 through 65535.

  Default: 1812

- **max-subscribers** *max_sessions*: Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.

  In 8.3 and earlier releases, *max_sessions* must be an integer from 0 through 3000000.

  In 9.0 and later releases, *max_sessions* must be an integer from 0 through 4000000.

- **source-context** *source_context*: Specifies the source context where RADIUS accounting requests are received.

  source_context must be an alphanumeric string of 1 through 79 characters.

  This keyword should be configured if the source of the RADIUS requests is in a different context then the IPSG service. If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

Usage

Use this command to bind the IPSG RADIUS Server service to a logical AAA interface and specify the number of allowed subscriber sessions. If the AAA interface is not located in this context, configure the **source-context** parameter.

Use the accounting and authentication proxy settings to enable RADIUS proxy server functionality on the IPSG. These commands are used when the NAS providing the RADIUS request messages is incapable of sending them to two separate devices. The IPSG in RADIUS Server mode proxies the RADIUS request and response messages while performing the user identification task in order to provide services to the session.

Example

The following command binds the service to a AAA interface with and IP address of *10.2.3.4* located in the source context named *aaa_ingress*:

```
bind address 10.2.3.4 source-context aaa_ingress
```

connection authorization

Configures the RADIUS authorization password that must be matched by the RADIUS accounting requests received by this service.

Product

IPSG

Privilege

Security Administrator, Administrator

Syntax

connection authorization [encrypted] password *password*

no connection authorization

no

Deletes the RADIUS authorization from the current IPSG RADIUS Server service.

[encrypted] password *password*

- **encrypted**: Specifies that the RADIUS authorization password is encrypted.
- **password** *password*: Specifies the password that must be matched by incoming RADIUS accounting requests.

  In 12.0 and earlier releases, *password* must be an alphanumeric string of 1 through 63 characters.

  In 12.2 and later releases, with encryption *password* must be an alphanumeric string of 1 through 132 characters. And without encryption, *password* must be an alphanumeric string of 1 through 63 characters.

Usage

The IPSG RADIUS server service does not terminate RADIUS user authentication so the user password is unknown.
Use this command to configure the authorization password that the RADIUS accounting requests must match in order for the service to examine and extract user information.

Example

The following command sets the RADIUS authorization password that must be matched by the RADIUS accounting requests sent to this service. The password must be encrypted and the example provided is the word "*secret*".

```
connection authorization encrypted password secret
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

profile

Configures the service to use an Access Point NAme (APN) or subscriber profiles.

Product

IPSG

Privilege

Security Administrator, Administrator

Syntax

```
profile { APN | subscriber }

default profile
```

default

Configures the default setting for this command.
Default: **APN**

APN

Specifies the service to support APN configuration required to enable Gx support.

subscriber

Specifies the service to support subscriber profile lookup.

Usage

Use this command to set the service to support APN profiles (supporting Gx through the enabling of **ims-auth-service**) or for basic subscriber profile lookup.

radius accounting

Specifies the IP address and shared secret of the RADIUS accounting client from which RADIUS accounting requests are received. The RADIUS client can be either the access gateway or the RADIUS accounting server depending on which device is sending accounting requests.

Product

IPSG

Privilege

Security Administrator, Administrator

Syntax

```
radius accounting { { client { ipv4/ipv6_address | ipv4/ipv6_address/mask } [ encrypted ]
key secret [ dictionary dictionary ] [ disconnect-message [ dest-port destination_port ]
] } | { interim create-new-call } }

no radius accounting client { ipv4/ipv6_address | ipv4/ipv6_address/mask }

default radius accounting interim create-new-call
```

no

Removes the RADIUS accounting client address identifier from the service.

ipv4/ipv6_address **|** *ipv4/ipv6_address/mask*

Specifies the IP address and, optionally, subnet mask of the RADIUS client from which RADIUS accounting requests are received.
ipv4/ipv6_address and *ipv6/ipv6_address/mask* are expressed in IPv4 dotted-decimal or IPv6 colon-separated notation with CIDR.
Up to 16 addresses can be configured.

dictionary *dictionary*

Specifies what dictionary database to use. The possible values for *dictionary* are described in the following table:

Dictionary	Description
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.
custom*X*	These are customized dictionaries. For information on custom dictionaries, please contact your Cisco account representative. *X* is the integer value of the custom dictionary.
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.
starent	This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.

Dictionary	Description
starent-835	This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.
starent-vsa1	This dictionary consists not only of the 3gpp2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary. ***Important:*** In 12.0 and later releases, no new attributes can be added to the **starent-vsa1** dictionary. If there are any new attributes to be added, these can only be added to the **starent** dictionary. For more information, please contact your Cisco account representative.
starent-vsa1-835	This dictionary consists not only of the 3gpp2-835 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary.

[encrypted] key *secret*

- **encrypted**: Specifies that the shared key between the RADIUS client and this service is encrypted.
- **key** *secret*: Specifies the shared key between the RADIUS client and this service.

  In 12.0 and earlier releases, *secret* must be an alphanumeric string of 1 through 127 characters and is case sensitive.

  In 12.2 and later releases, with encryption *secret* must be an alphanumeric string of 1 through 236 characters and is case sensitive. And, without encryption *secret* must be an alphanumeric string of 1 through 127 characters and is case sensitive

disconnect-message [dest-port *destination_port* **]**

Specifies sending disconnect message.
dest-port *destination_port*: Specifies the port number to which the disconnect message must be sent. *destination_port* must be an integer from 1 through 65535.

interim create-new-call

Enables the ability to create a new session upon receipt of a RADIUS interim message. Default: Disabled

Usage

Use this command to configure the communication with the RADIUS client from which RADIUS accounting requests are received.

Example

The following command configures the service to communicate with a RADIUS client with an IP address of *10.2.3.4* and an encrypted shared secret of *secret_1234*:

```
radius accounting client 10.2.3.4 encrypted key secret_1234
```

radius dictionary

Configures the RADIUS database dictionary for use with the IPSG service.

Product

IPSG

Privilege

Security Administrator, Administrator

Syntax

radius dictionary *dictionary*

default radius dictionary

dictionary *dictionary*

Default: **starent-vsa1**
Specifies what dictionary database to use. The possible values for *dictionary* are described in the table that follows:

Dictionary	Description
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.
custom*XX*	These are customized dictionaries. For information on custom dictionaries, please contact your Cisco account representative. *XX* is the integer value of the custom dictionary.
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.
starent	This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.
starent-835	This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.
starent-vsa1	This dictionary consists not only of the 3gpp2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary.
starent-vsa1-835	This dictionary consists not only of the 3gpp2-835 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary.

Usage

Use this command to specify the RADIUS database dictionary to use for the IPSG service.

Example

The following command configures the IPSG service to use the *custom10* RADIUS database dictionary:

```
radius dictionary custom10
```

setup-timeout

Configures a timeout value for IPSG session set up attempts.

Product

IPSG

Privilege

Security Administrator, Administrator

Syntax

setup-timeout *setup_timeout*

default setup-timeout

setup_timeout

Specifies the time period (in seconds) IPSG session setup attempt is allowed to continue before being terminated.
setup_timeout must be an integer from 1 through 1000000.
Default: 60

Usage

Use this command to prevent IPSG session set up attempts from continuing without termination.

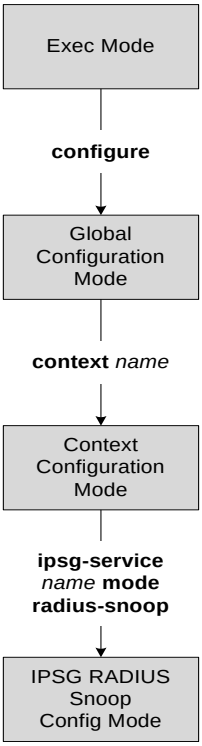
Example

The following command sets the session setup timeout to *20* seconds:

```
setup-timeout 20
```

Chapter 159
IPSG RADIUS Snoop Configuration Mode Commands

The IP Services Gateway (IPSG) RADIUS Snoop Configuration Mode is used to create and configure IPSG services within the current context. The IPSG RADIUS Snoop Mode configures the system to inspect RADIUS accounting requests on the way to the RADIUS accounting server and extract user information.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

bind

Configures the service to accept data on any interface configured in the context. Optionally allows the system to limit the number of sessions processed by this service.

Product

IPSG

Privilege

Security Administrator, Administrator

Syntax

bind [max-subscribers *max_sessions* **]**

no bind

no

If previously configured, deletes the binding configuration for the service.

max-subscribers *max_sessions*

Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.
In 8.3 and earlier releases, *max_sessions* must be an integer from 0 through 3000000.
In 9.0 and later releases, *max_sessions* must be an integer from 0 through 4000000.

Usage

Use this command to initiate the service and begin accepting data on any interface configured in the context.

Example

The following command prepares the system to receive subscriber sessions on any interface in the context and limits the sessions to *10000*:

```
bind max-subscribers 10000
```

connection authorization

Sets the RADIUS authorization password that must be matched by the RADIUS accounting requests "snooped" by this service.

Product

IPSG

Privilege

Security Administrator, Administrator

Syntax

connection authorization [encrypted] password *password*

no connection authorization

---

no

Deletes the RADIUS connection authorization configuration from the current IPSG RADIUS snoop service.

[encrypted] password *password*

- **encrypted**: Specifies that the received RADIUS authorization password is encrypted.
- **password** *password*: Specifies the password that must be matched by incoming RADIUS accounting requests.

  In 12.0 and earlier releases, *password* must be an alphanumeric string of 1 through 63 characters.

  In 12.2 and later releases, with encryption *password* must be an alphanumeric string of 1 through 132 characters. And, without *password* must be an alphanumeric string of 1 through 63 characters.

Usage

RADIUS accounting requests being examined by the IPSG RADIUS snoop service are destined for a RADIUS Accounting Server. Since the "snoop" service does not terminate user authentication, the user password is unknown.
Use this command to configure the authorization password that the RADIUS accounting requests must match in order for the service to examine and extract user information.

Example

The following command sets the RADIUS authorization password that must be matched by the RADIUS accounting requests "snooped" by this service. The password must be encrypted and the example provided is the word "*secret*".

```
connection authorization encrypted password secret
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

radius

Specifies the RADIUS accounting servers where accounting requests are sent after being "inspected" by this service.

Product

IPSG

Privilege

Security Administrator, Administrator

Syntax

[no] radius { accounting server *ipv4/ipv6_address* **[port** *port_number* **| source-context** *context_name* **] | dictionary { 3gpp2 | 3gpp2-835 | custom** *XX* **| standard | starent | starent-835 | starent-vsa1 | starent-vsa1-835 } }**

no

Removes the RADIUS accounting server identifier from this service.

radius accounting server *ipv4/ipv6_address*

Specifies the IP address of a RADIUS accounting server where accounting requests are sent after being "snooped" by this service in IPv4 dotted-decimal or IPv6 colon-separated notation.
Up to 16 addresses can be configured.

port *port_number*

Specifies the port number of the RADIUS Accounting Server where accounting requests are sent after being "snooped" by this service.
port_number must be an integer from 1 through 65535.
Default: 1813

source-context *context_name*

Specifies the source context where RADIUS accounting requests are received.
context_name must be an alphanumeric string of 1through 79 characters.
If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

dictionary { 3gpp2 | 3gpp2-835 | custom *XX* **| standard | starent | starent-835 | starent-vsa1 | starent-vsa1-835 }**

Specifies what dictionary to use. The possible values are described in the following table:

Dictionary	Description
3gpp	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in 3GPP 32.015.
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.

Dictionary	Description
custom*XX*	These are customized dictionaries. For information on custom dictionaries, please contact your Cisco account representative. *XX* is the integer value of the custom dictionary.
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.
starent	This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.
starent-835	This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.
starent-vsa1	This dictionary consists not only of the 3gpp2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary.
starent-vsa1-835	This dictionary consists not only of the 3gpp2-835 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary.

Usage

Use this command to specify the RADIUS Accounting Servers where accounting requests are sent after being snooped by this service.

Example

The following command specifies the IP address (*10.2.3.4*) of a RADIUS Accounting Server whose accounting requests are to be “snooped”, and the source context (*aaa_ingress*) where the requests are received on the system:

```
radius accounting server 10.2.3.4 source-context aaa_ingress
```

setup-timeout

Configures a timeout value for IPSG session setup attempts.

Product

IPSG

Privilege

Security Administrator, Administrator

Syntax

setup-timeout *setup_timeout*

default setup-timeout

setup_timeout

Specifies the period of time (in seconds) the IPSG session setup is allowed to continue before the setup attempt is terminated.
setup_timeout must be an integer from 1 through 1000000.
Default: 60

Usage

Use this command to prevent IPSG session setup attempts from continuing without termination.

Example

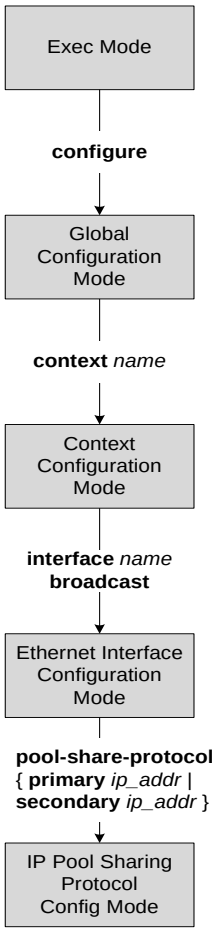
The following command configures the session setup timeout setting to *20* seconds:

```
setup-timeout 20
```

Chapter 160
IPSP Configuration Mode Commands

The IPSP Configuration Mode is used to configure properties for the IP Pool Sharing Protocol (IPSP). System-based HA services use IPSP during an offline-software upgrade to avoid the assignment of duplicate IP addresses to sessions while allowing them to maintain the same address, and to preserve network capacity

Important: For information on configuring and using IPSP refer to the System Administration and Configuration Guide.



dead-interval

Configures the retry time to connect to the remote system for the IP Pool Sharing Protocol.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

dead-interval*seconds*

[no | default] dead-interval

no

Disables the dead interval. On loss of connectivity to the remote system, no retries are attempted and the remote system is marked dead immediately on failure.

default

Resets the dead interval to the default of 3600 seconds.

seconds

Default: 3600 seconds
The amount of time in seconds to wait before retrying the remote system. *seconds* must be an integer from 25 through 259200.

Usage

Use this command to set the amount of time to wait before retrying to connect with the remote system for the IP pool sharing protocol.

Example

Use the following command to set the interval to 180 seconds (3 minutes):
dead-interval 180

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

reserved-free-percentage

This command is used to set the amount of free addresses reserved for use on the primary HA.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

reserved-free-percentage *value*

default reserved-free-percentage

value

Default: 100
value specifies the percentage of free addresses reserved for the use on the primary HA for IP pool sharing during upgrade. It must be an integer from 0 through 100.

Usage

This command is used with **pool-sharing-protocol active mode** on the primary HA. Before using this command, **pool-sharing-protocol** in the Ethernet Interface Configuration Mode must be configured. For more information, refer to the *Ethernet Interface Configuration Mode Commands* chapter in this guide.

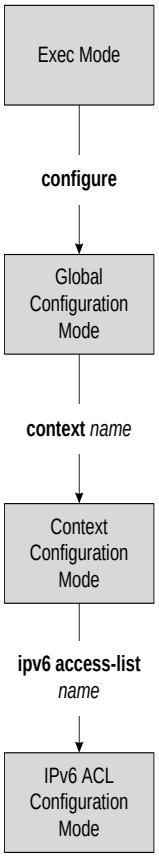
Example

To reserve 40 percent of free addresses in primary HA for IP pool sharing, enter the following command:

```
reserved-free-percentage 40
```

Chapter 161
IPv6 ACL Configuration Mode Commands

The IPv6 Access Control List Configuration Mode is used to create and manage IPv6 access privileges.



deny/permit (by source IP address masking)

Used to filter subscriber sessions based on the IPv6 address mask sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

{ deny | permit } [log] *source_address source_wildcard*

after { deny | permit } [log] *source_address source_wildcard*

before { deny | permit } [log] *source_address source_wildcard*

no { deny | permit } [log] *source_address source_wildcard*

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

Usage

Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rules as it does not require a rule for each source and destination pair.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Example

The following command defines two rules with the second logging filtered packets:

```
permit 2001:4A2B::1f3F

deny log 2001:4A2B::1f3F
```

The following sets the insertion point to before the first rule defined above:

```
before permit 2001:4A2B::1f3F
```

The following command sets the insertion point after the second rule defined above:

```
after deny log 2001:4A2B::1f3F
```

The following deletes the first rule defined above:

```
no permit 2001:4A2B::1f3F
```

deny/permit (any)

Used to filter subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
{ deny | permit } [ log ] any

after { deny | permit } [ log ] any

before { deny | permit } [ log ] any

no { deny | permit } [ log ] any
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

any

Indicates all packets will match the filter regardless of source and/or destination.

Usage

Define a catch all rule to place at the end of the list of rules.

Important: It is suggested that any rule which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines two rules with the second logging filtered packets:

```
permit any

deny log any
```

The following sets the insertion point to before the first rule defined above:

```
before permit any
```

The following command sets the insertion point after the second rule defined above:

```
after deny log any
```

The following deletes the first rule defined above:

```
no permit any
```

deny/permit (by host IP address)

Used to filter subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

{ deny | permit } [log] host *source_host_address*

after { deny | permit } [log] host *source_host_address*

before { deny | permit } [log] host *source_host_address*

no { deny | permit } [log] host *source_host_address*

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

Usage

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines two rules with the second logging filtered packets:

```
permit host 2001:4A2B::1f3F

deny log host 2001:4A2B::1f3F
```

The following sets the insertion point to before the first rule defined above:

```
before permit host 2001:4A2B::1f3F
```

The following command sets the insertion point after the second rule defined above:

```
after deny log host 2001:4A2B::1f3F
```

The following deletes the first rule defined above:

```
no permit host 2001:4A2B::1f3F
```

deny/permit (by source ICMP packets)

Used to filter subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
{ deny | permit } [ log ] icmp { source_address source_wildcard | any | host
source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [
icmp_type [ icmp_code ] ]

after { deny | permit } [ log ] icmp { source_address source_wildcard | any | host
source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [
icmp_type [ icmp_code ] ]

before { deny | permit } [ log ] icmp { source_address source_wildcard | any | host
source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [
icmp_type [ icmp_code ] ]

no { deny | permit } [ log ] icmp { source_address source_wildcard | any | host
source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [
icmp_type [ icmp_code ] ]
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type is an integer from 0 through 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type is an integer from 0 through 255.

Usage

Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk. The IP filtering allows flexible controls for pairs of individual hosts or groups by IP masking which allows the filtering of entire subnets if necessary.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines two rules with the second logging filtered packets:

```
permit icmp host 2001:4A2B::1f3F4 any 168

deny log icmp 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410 168 11
```

The following sets the insertion point to before the first rule defined above:

```
before permit icmp host 2001:4A2B::1f3F any 168
```

The following command sets the insertion point after the second rule defined above:

```
after deny log icmp 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410
168 11
```

The following deletes the first rule defined above:

```
no permit icmp host 2001:4A2B::1f3F any 168
```

deny/permit (by IP packets)

Used to filter subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

{ deny | permit } [log] ip { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [fragment] [protocol*num*]

after { deny | permit } [log] ip { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [fragment] [protocol*num*]

before { deny | permit } [log] ip { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [fragment] [protocol*num*]

no { deny | permit } [log] ip { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [fragment] [protocol*num*]

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: indicates the rule, when matched, drops the corresponding packets.
- **permit**: indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

fragment

Indicates packet filtering is to be applied to IP packet fragments only.

protocol *num*

Indicates that the packet filtering is to be applied to a specific protocol number.
num can be any integer ranging from 0 to 255.

Usage

Block IP packets when the source and destination are of interest.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines two rules with the second logging filtered packets:

```
permit ip host 2001:4A2B::1f3F any fragment

deny log ip 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410
```

The following sets the insertion point to before the first rule defined above:

```
before permit ip host 2001:4A2B::1f3F any fragment
```

The following command sets the insertion point after the second rule defined above:

```
after deny log ip 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410
```

The following deletes the first rule defined above:

```
no permit ip host 2001:4A2B::1f3F any fragment
```

deny/permit (by TCP/UDP packets)

Used to filter subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

{ deny | permit } [log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dst_port*] }

after { deny | permit } [log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dst_port*] }

before { deny | permit } [log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dst_port*] }

no { deny | permit } [log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dst_port*] }

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

tcp | udp

Specifies the filter is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Filter applies to TPC packets.
- **udp**: Filter applies to UDP packets.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to an integer from 0 through 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to an integer from 0 through 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
dest_port must be configured to an integer from 0 through 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered. *dest_port* must be configured to an integer from 0 through 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. *dest_port* must be configured to an integer from 0 through 65535.

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines four rules with the second and fourth rules logging filtered packets:

```
permit tcp host 2001:4A2B::1f3F any

deny log udp 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410

permit tcp host 2001:4A2B::1f3F gt 1023 any
```

The following sets the insertion point to before the first rule defined above:

```
before permit tcp host 2001:4A2B::1f3F any
```

The following command sets the insertion point after the second rule defined above:

```
after deny log udp 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410
```

The following deletes the third rule defined above:

```
no permit tcp host 2001:4A2B::1f3F gt 1023 any
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

readdress server

Alter the destination address and port number in TCP or UDP packet headers to redirect packets to a different server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

redirect_address

The IP address to which the IP packets are redirected. TCP or UDP packet headers are rewritten to contain the new destination address. This must expressed in IPv6 colon-separated notation.

port *port_number*

The number of the port at the redirect address where the packets are sent. TCP or UDP packet headers are rewritten to contain the new destination port number.

tcp | udp

Specifies the redirect is to be applied to the IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TCP packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to an integer from 0 through 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to an integer from 0 through 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be configured to an integer from 0 through 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered. *dest_port* must be configured to an integer from 0 through 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. *dest_port* must be configured to an integer from 0 through 65535.

Usage

Use this command to define a rule that redirects packets to a different destination address. The TCP and UDP packet headers are modified with the new destination address and destination port.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the server at *fe80::c0a8:a04*, UDP packets coming from any host with a destination of any host are matched:

```
readdress server fe80::c0a8:a04 udp any any
```

The following sets the insertion point to before the rule defined above:

```
before readdress server fe80::c0a8:a04 udp any any
```

The following deletes the rule defined above:

```
no readdress server fe80::c0a8:a04 udp any any
```

redirect context (by IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect context *context_id* **[log]** *source_address source_wildcard*

after redirect context *context_id* **[log]** *source_address source_wildcard*

before redirect context *context_id* **[log]** *source_address source_wildcard*

no redirect context *context_id* **[log]** *source_address source_wildcard*

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

Specifies the context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

Filters by the IP address(es) from which the packet originated. This option filters all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

Filters packets for a group of addresses specified in conjunction with the *source_address* option.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

Usage

Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of redirect rules as it does not require a rule for each source and destination pair.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of *23* and the source IP and wildcard of *2002::c6a2:1600* and *2002::c6a2:1600*:

```
redirect context 23 2002::c6a2:1600 2002::c6a2:1600
```

The following sets the insertion point to before the first rule defined above:

```
before redirect context 23 2002::c6a2:1600 2002::c6a2:1600
```

The following command sets the insertion point after the second rule defined above:

```
after redirect context 23 2002::c6a2:1600 2002::c6a2:1600
```

The following deletes the first rule defined above:

```
no redirect context 23 2002::c6a2:1600 2002::c6a2:1600
```

redirect context (any)

Used to redirect subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect context *context_id* **[log] any**

after redirect context *context_id* **[log] any**

before redirect context *context_id* **[log] any**

no redirect context *context_id* **[log] any**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage

Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

Important: It is suggested that any rule which is added to be a catch all should also have the log option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of *23* and any source IP:

```
redirect context 23 any
```

The following sets the insertion point to before the first rule defined above:

```
before redirect context 23 any
```

The following command sets the insertion point after the second rule defined above:

```
after redirect context 23 any
```

The following deletes the first rule defined above:

```
no redirect context 23 any
```

redirect context (by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect context *context_id* **[log] host** *source_ip_address*

after redirect context *context_id* **[log] host** *source_ip_address*

before redirect context *context_id* **[log] host** *source_ip_address*

no redirect context *context_id* **[log] host** *source_ip_address*

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated notation.

Usage

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of *23* and a host IP address of *fe80::c0a8:c80b*:

```
redirect context 23 host fe80::c0a8:c80b
```

The following sets the insertion point to before the first rule defined above:

```
before redirect context 23 host fe80::c0a8:c80b
```

The following command sets the insertion point after the second rule defined above:

```
after redirect context 23 host fe80::c0a8:c80b
```

The following deletes the first rule defined above:

```
no redirect context 23 host fe80::c0a8:c80b
```

redirect context (by source ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect context *context_id* **[log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

after redirect context *context_id* **[log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

before redirect context *context_id* **[log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

no redirect context *context_id* **[log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. Type is an integer from 0 through 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered type is an integer from 0 through 255.

Usage

Define a rule to block ICMP packets which can be used for address resolution and possibly be a security risk. The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of *23*, and ICMP packets coming from the host with the IP address *2002::c6a2:6419*:

```
redirect context 23 icmp host 2002::c6a2:6419
```

The following sets the insertion point to before the first rule defined above:

```
before redirect context 23 icmp host 2002::c6a2:6419
```

The following command sets the insertion point after the second rule defined above:

```
after redirect context 23 icmp host 2002::c6a2:6419
```

The following deletes the first rule defined above:

```
no redirect context 23 icmp host 2002::c6a2:6419
```

redirect context (by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect context *context_id* **[log] ip { *source_address source_wildcard* | any | host** *source_host_address* **} { *dest_address dest_wildcard* | any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**

after redirect context *context_id* **[log] ip { *source_address source_wildcard* | any | host** *source_host_address* **} { *dest_address dest_wildcard* | any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**

before redirect context *context_id* **[log] ip { *source_address source_wildcard* | any | host** *source_host_address* **} { *dest_address dest_wildcard* | any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**

no redirect context *context_id* **[log] ip { *source_address source_wildcard* | any | host** *source_host_address* **} { *dest_address dest_wildcard* | any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

protocol *num*

Indicates that the packet filtering is to be applied to a specific protocol number.
num is an integer from 0 through 255.

Usage

Block IP packets when the source and destination are of interest.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of *23*, and IP packets coming from the host with the IP address *2002::c6a2:6419*, and fragmented packets for any destination are matched:

```
redirect context 23 ip host 2002::c6a2:6419 any fragment
```

The following sets the insertion point to before the first rule defined above:

```
before redirect context 23 ip host 198.162.100.25 any fragment
```

The following command sets the insertion point after the second rule defined above:

```
after redirect context 23 ip host 2002::c6a2:6419 any fragment
```

The following deletes the first rule defined above:

```
no redirect context 23 ip host 2002::c6a2:6419 any fragment
```

redirect context (by TCP/UDP packets)

Used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect context *context_id* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dst_port*] }**

after redirect context *context_id* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dst_port*] }**

before redirect context *context_id* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dst_port*] }**

no redirect context *context_id* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dst_port*] }**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to an integer from 0 through 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to an integer from 0 through 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
dest_port must be configured to an integer from 0 through 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.
dest_port must be configured to an integer from 0 through 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. *dest_port* must be configured to an integer from 0 through 65535.

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of *23*, and UDP packets coming from any host are matched:

```
redirect context 23 udp any
```

The following sets the insertion point to before the rule defined above:

```
before redirect context 23 udp any
```

The following command sets the insertion point after the rule defined above:

```
after redirect context 23 udp any
```

The following deletes the rule defined above:

```
no redirect context 23 udp any
```

redirect css delivery-sequence

This is a restricted command. In StarOS 9.0 and later, this command is obsoleted.

redirect css service (any)

Used to redirect subscriber sessions based on any packet received with Content Service Steering (CSS) enabled. This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *svc_name* **[log] any**

after redirect css service *svc_name* **[log] any**

before redirect css service *svc_name* **[log] any**

no redirect css service *svc_name* **[log] any**

after

Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definitions which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the CSS service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.
svc_name must be a string of 1 through 15 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage

Define a catch all rule definitions to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

Important: It is suggested that any rule definition which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

Important: A maximum of 16 rule definitions can be configured per ACL.

Important: Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the CSS service with the name *css-svc1* and any source IP:

```
redirect css service css-svc1 any
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 any
```

The following command sets the insertion point after the second rule definitions above:

```
after redirect css service css-svc1 any
```

The following deletes the first rule definition above:

```
no redirect css service css-svc1 any
```

redirect css service (by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *svc_name* **[log] host** *source_host_address*

after redirect css service *svc_name* **[log] host** *source_host_address*

before redirect css service *svc_name* **[log] host** *source_host_address*

no redirect css service *svc_name* **[log] host** *source_host_address*

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.
svc_name must be an alphanumeric string of 1 through 15 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated notation.

Usage

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the CSS service with the name *css-svc1* and a host IP address of *fe80::c0a8:c80b*:

```
redirect css service css-svc1 host fe80::c0a8:c80b
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 host fe80::c0a8:c80b
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service css-svc1 host fe80::c0a8:c80b
```

The following deletes the first rule definition above:

```
no redirect css service css-svc1 host fe80::c0a8:c80b
```

redirect css service (by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect css service svc_name [ log ] icmp { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [icmp_type [ icmp_code ] ]

after redirect css service svc_name [ log ] icmp { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [icmp_type [ icmp_code ] ]

before redirect css service svc_name [ log ] icmp { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [icmp_type [ icmp_code ] ]

no redirect css service svc_name [ log ] icmp { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [icmp_type [ icmp_code ] ]
```

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

`css service` *`svc_name`*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **`show css service all`** command to display the names of all configured charging services.
`svc_name` must be an alphanumeric string of 1 through 15 characters.

`log`

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

`source_address`

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *`source_wildcard`* parameter.

`source_wildcard`

This option is used in conjunction with the *`source_address`* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *`source_address`* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *`source_address`* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

`any`

Specifies that the rule definition applies to all packets.

`host`

Specifies that the rule definition applies to a specific host as determined by its IP address.

`source_host_address`

The IP address of the source host to filter against expressed in IPv6 colon-separated notation.

`dest_host_address`

The IP address of the destination host to filter against expressed in IPv6 colon-separated notation.

`dest_address`

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *`dest_wildcard`* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value from 0 through 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type is an integer from 0 through 255.

Usage

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.
The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the CSS service named *css-svc1*, and ICMP packets coming from the host with the IP address *2002::c6a2:6419*:

```
redirect css service css-svc1 icmp host 2002::c6a2:6419
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 icmp host 2002::c6a2:6419
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service css-svc1 icmp host 2002::c6a2:64195
```

The following deletes the first rule definition above:

```
no redirect css service css-svc1 icmp host 2002::c6a2:6419
```

redirect css service (by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect css service svc_name [ log ] ip { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ fragment ]

after redirect css service svc_name [ log ] ip { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ fragment ]

before redirect css service svc_name [ log ] ip { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ fragment ]

no redirect css service svc_name [ log ] ip { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ fragment ]
```

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

`css service` *`svc_name`*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **`show css service all`** command to display the names of all configured CSS services.
`svc_name` must be an alphanumeric string of 1 through 15 characters.

`log`

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

`source_address`

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *`source_wildcard`* parameter.

`source_wildcard`

This option is used in conjunction with the *`source_address`* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *`source_address`* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *`source_address`* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

`any`

Specifies that the rule definition applies to all packets.

`host`

Specifies that the rule definition applies to a specific host as determined by its IP address.

`source_host_address`

The IP address of the source host to filter against expressed in IPv6 colon-separated notation.

`dest_host_address`

The IP address of the destination host to filter against expressed in IPv6 colon-separated notation.

`dest_address`

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *`dest_wildcard`* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

Usage

Block IP packets when the source and destination are of interest.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the CSS service named *css-svc1*, and IP packets coming from the host with the IP address *2002::c6a2:6419*, and fragmented packets for any destination are matched:

```
redirect css service css-svc1 ip host 2002::c6a2:6419 any fragment
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 ip host 2002::c6a2:6419 any fragment
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service css-svc1 ip host 2002::c6a2:6419 any fragment
```

The following deletes the first rule definition above:

```
no redirect css service css-svc1 ip host 2002::c6a2:6419 any fragment
```

redirect css service (by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *svc_name* **[log]** *source_address source_wildcard*

after redirect css service *svc_name* **[log]** *source_address source_wildcard*

before redirect css service *svc_name* **[log]** *source_address source_wildcard*

no redirect css service *svc_name* **[log]** *source_address source_wildcard*

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.
svc_name must be an alphanumeric string of 1 through 15 characters.

log

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

Usage

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Important: A maximum of 16 rule definitions can be configured per ACL.

Example

The following command defines a rule definition to redirect packets to a CSS service named *css-svc1*:

```
redirect css service css=svc1 2002::c6a2:6419
```

redirect css service (by TCP/UDP packets)

Used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *svc_name* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port* | range *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port* | range *start_dest_port end_dest_port*] }**

after redirect css service *svc_name* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port* | range *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port* | range *start_dest_port end_dest_port*] }**

after redirect css service *svc_name* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port* | range *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port* | range *start_dest_port end_dest_port*] }**

no redirect css service *svc_name* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port* | range *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port* | range *start_dest_port end_dest_port*] }**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured charging services.
svc_name must be an alphanumeric string of 1 through 15 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to an integer from 0 to 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to an integer from 0 to 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to an integer from 0 to 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to an integer from 0 to 65535.

range *start_source_port end_source_port*

Specifies that all source TCP ports within a specific range are to be filtered.
start_source_port is the initial port in the range and *end_source_port* is the final port in the range.
Both *start_source_port* and *end_source_port* can be configured to an integer from 0 to 65535.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to an integer from 0 to 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
dest_port must be configured to an integer from 0 to 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.
dest_port must be configured to an integer from 0 to 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.
dest_port must be configured to an integer from 0 to 65535.

range *start_dest_port end_dest_port*

Specifies that all destination TCP ports within a specific range are to be filtered.
start_dest_port is the initial port in the range and *end_dest_port* is the final port in the range.
Both *start_dest_port* and *end_dest_port* can be configured to an integer from 0 to 65535

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the CSS service named *css-svc1*, and UDP packets coming from any host are matched:

```
redirect css service css-svc1 udp any
```

The following sets the insertion point to before the rule definition above:

```
before redirect css service css-svc1 udp any
```

The following command sets the insertion point after the rule definition above:

```
after redirect css service css-svc1 udp any
```

The following deletes the rule definition above:

```
no redirect css service css-svc1 udp any
```

redirect css service (for downlink, any)

Used to redirect subscriber sessions based on any packet received in the downlink (from the Mobile Node) direction. This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect css service svc_name [ log ] downlink any

after redirect css service svc_name [ log ] downlink any

before redirect css service svc_name [ log ] downlink any

no redirect css service svc_name [ log ] downlink any
```

after

Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.
svc_name must be an alphanumeric string of 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage

Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

Important: It is suggested that any rule definition which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

Important: A maximum of 16 rule definitions can be configured per ACL.

Important: Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the CSS service with the name *css-svc1* and any source IP:

```
redirect css service css-svc1 downlink any
```

The following sets the insertion point to before the first rule definition above:

```
before redirect service css-svc1 downlink any
```

The following command sets the insertion point after the second rule definition above:

```
after redirect service css-svc1 downlink any chgsvc1 downlink any
```

The following deletes the first rule definition above:

```
no redirect service css-svc1 downlink any
```

redirect css service (for downlink, by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address in the downlink (from the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *svc_name* **[log] downlink host** *source_host_address*

after redirect css service *svc_name* **[log] downlink host** *source_host_address*

before redirect css service *svc_name* **[log] downlink host** *source_host_address*

no redirect css service *svc_name* **[log] downlink host** *source_host_address*

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.
svc_name must be an alphanumeric string of 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated notation.

Usage

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *css-svc1* and a host IP address of *fe80::c0a8:c80b*:

```
redirect service css-svc1 downlink host fe80::c0a8:c80b
```

The following sets the insertion point to before the first rule definition above:

```
before redirect service css-svc1 downlink host fe80::c0a8:c80b
```

The following command sets the insertion point after the second rule definition above:

```
after redirect service css-svc1 downlink host fe80::c0a8:c80b
```

The following deletes the first rule definition above:

```
no redirect service css-svc1 downlink host fe80::c0a8:c80b
```

redirect css service (for downlink, by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets in the downlink (from the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *svc_name* **[log] downlink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]]**

after redirect css service *svc_name* **[log] downlink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]]**

before redirect css service *svc_name* **[log] downlink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]]**

no redirect css service *svc_name* **[log] downlink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.
svc_name must be an alphanumeric string of 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value from 0 through 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value from 0 through 255.

Usage

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.
The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *css-svc1*, and ICMP packets coming in the downlink (from the Mobile Node) direction from the host with the IP address *2002::c6a2:6419*:

```
redirect css service css-svc1 downlink icmp host 2002::c6a2:6419
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 downlink icmp host 2002::c6a2:6419
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service css-svc1 downlink icmp host 2002::c6a2:6419
```

The following deletes the first rule definition above:

```
no redirect css service css-svc1 downlink icmp host 2002::c6a2:6419
```

redirect css service (for downlink, by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets in the downlink (from the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *svc_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

after redirect css service *svc_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

before redirect css service *svc_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

no redirect css service *svc_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

`css service` *`svc_name`*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **`show css service all`** command to display the names of all configured CSS services.
`svc_name` must be a string of 1 through 15 characters.

`downlink`

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

`log`

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

`source_address`

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *`source_wildcard`* parameter.

`source_wildcard`

This option is used in conjunction with the *`source_address`* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *`source_address`* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *`source_address`* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

`any`

Specifies that the rule definition applies to all packets.

`host`

Specifies that the rule definition applies to a specific host as determined by its IP address.

`source_host_address`

The IP address of the source host to filter against expressed in IPv6 colon notation.

`dest_host_address`

The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

Usage

Block IP packets when the source and destination are of interest.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *css-svc1*, and downlink IP packets coming from the host with the IP address *2002::c6a2:6419*, and fragmented packets for any destination are matched:

```
redirect css service css-svc1 downlink ip host 2002::c6a2:6419 any
fragment
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 downlink ip host 2002::c6a2:6419 any
fragment
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service css-svc1 downlink ip host 2002::c6a2:6419 any
fragment
```

The following deletes the first rule definition above:

```
no redirect css service css-svc1 downlink ip host 2002::c6a2:6419 any
fragment
```

redirect css service (for downlink, by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source in the downlink (from the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *svc_name* **[log] downlink** *source_address source_wildcard*

after redirect css service *svc_name* **[log] downlink** *source_address source_wildcard*

before redirect css service *svc_name* **[log] downlink** *source_address source_wildcard*

no redirect css service *svc_name* **[log] downlink** *source_address source_wildcard*

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.
svc_name must be an alphanumeric string of 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

Usage

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Important: A maximum of 16 rule definitions can be configured per ACL.

Example

The following command defines a rule definition to redirect packets to a charging service named *css-svc1*:

```
redirect css service css-svc1 donwlink fe80::c0a8:a04
```

redirect css service (for downlink, by TCP/UDP packets)

Used to redirect subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the downlink (from the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *svc_name* **[log] downlink { tcp | udp } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

after redirect css service *svc_name* **[log] downlink { tcp | udp } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

after redirect css service *svc_name* **[log] downlink { tcp | udp } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

no redirect css service *svc_name* **[log] downlink { tcp | udp } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.
svc_name must be an alphanumeric string of 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to an integer value from 0 to 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

range *start_source_port end_source_port*

Specifies that all source TCP ports within a specific range are to be filtered.
start_source_port is the initial port in the range and *end_source_port* is the final port in the range.
Both *start_source_port* and *end_source_port* can be configured to an integer value from 0 to 65535.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

range *start_dest_port end_dest_port*

Specifies that all destination TCP ports within a specific range are to be filtered.
start_dest_port is the initial port in the range and *end_dest_port* is the final port in the range.
Both *start_dest_port* and *end_dest_port* can be configured to an integer value from 0 to 65535.

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *css-svc1*, and UDP packets coming from any host are matched:

```
redirect css service css-svc1 downlink udp any
```

The following sets the insertion point to before the rule definition above:

```
before redirect css service css-svc1 downlink udp any
```

The following command sets the insertion point after the rule definition above:

```
after redirect css service css-svc1 downlink udp any
```

The following deletes the rule definition above:

```
no redirect css service css-svc1 downlink udp any
```

redirect css service (for uplink, any)

Used to redirect subscriber sessions based on any packet received in the uplink (to the Mobile Node) direction. This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *svc_name* **[log] uplink any**

after redirect css service *svc_name* **[log] uplink any**

before redirect css service *svc_name* **[log] uplink any**

no redirect css service *svc_name* **[log] uplink any**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.
svc_name must be an alphanumeric string of 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage

Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

Important: It is suggested that any rule definition which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

Important: A maximum of 16 rule definitions can be configured per ACL.

Important: Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *css-svc1* and any source IP:

```
redirect css service css-svc1 uplink any
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 uplink any
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service css-svc1 uplink any
```

The following deletes the first rule definition above:

```
no redirect css service css-svc1 uplink any
```

redirect css service (for uplink, by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address in the uplink (to the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *svc_name* **[log] uplink host** *source_host_address*

after redirect css service *svc_name* **[log] uplink host** *source_host_address*

before redirect css service *svc_name* **[log] uplink host** *source_host_address*

no redirect css service *svc_name* **[log] uplink host** *source_host_address*

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

after

Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.

svc_name must ben alphanumeric string of 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

Usage

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *css-svc1* and a host IP address of *fe80::c0a8:c80b*:

```
redirect service css-svc1 uplink host fe80::c0a8:c80b
```

The following sets the insertion point to before the first rule definition above:

```
before redirect service css-svc1 uplink host fe80::c0a8:c80b
```

The following command sets the insertion point after the second rule definition above:

```
after redirect service css-svc1 uplink host fe80::c0a8:c80b
```

The following deletes the first rule definition above:

```
no redirect service css-svc1 uplink host fe80::c0a8:c80b
```

redirect css service (for uplink, by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets in the uplink (to the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *svc_name* **[log] uplink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]]**

---

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

---

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

---

no

Removes the rule definition which exactly matches the options specified.

---

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.
svc_name must be an alphanumeric string of 1 through 15 characters.

---

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.

- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value from 0 through 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value from 0 through 255.

Usage

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.
The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and ICMP packets in the uplink (to the Mobile Node) direction from the host with the IP address *198.162.100.25*:

```
redirect css service chgsvc1 uplink icmp host 198.162.100.25
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service chgsvc1 uplink icmp host 198.162.100.25
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service chgsvc1 uplink icmp host 198.162.100.25
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 uplink icmp host 198.162.100.25
```

redirect css service (for uplink, by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets in the uplink (to the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
redirect css service svc_name [ log ] uplink ip { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ fragment ]

after redirect css service svc_name [ log ] uplink ip { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ fragment ]

before redirect css service svc_name [ log ] uplink ip { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ fragment ]

no redirect css service svc_name [ log ] uplink ip { any | host source_host_address |
source_address source_wildcard } { any | host dest_host_address | dest_address
dest_wildcard } [ fragment ]
```

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
svc_name must be a string of 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

Usage

Block IP packets when the source and destination are of interest.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and uplink IP packets going to the host with the IP address *198.162.100.25*, and fragmented packets for any destination are matched:

```
redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

The following sets the insertion point to before the first rule definition above:

```
redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service chgsvc1 uplink ip host 198.162.100.25 any
fragment
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 uplink ip host 198.162.100.25 any
fragment
```

redirect css service (for uplink, by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source in the uplink (to the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *svc_name* **[log] uplink** *source_address source_wildcard*

---

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

---

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

---

no

Removes the rule definition which exactly matches the options specified.

---

css service *svc_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
svc_name must be a string of 1 through 15 characters.

---

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

---

log

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

---

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Usage

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Example

The following command defines a rule definition to redirect packets to a charging service named *chgsvc1*:

```
redirect css service chgsvc1 uplink 1:1:1:1:1:1:1:1
```

redirect css service (for uplink, by TCP/UDP packets)

Used to redirect subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the uplink (to the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect css service *svc_name* **[log] uplink { tcp | udp } { { *source_address source_wildcard* | **any** | *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

after redirect css service *svc_name* **[log] uplink { tcp | udp } { { *source_address source_wildcard* | **any** | *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

before redirect css service *svc_name* **[log] uplink { tcp | udp } { { *source_address source_wildcard* | **any** | *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

no redirect css service *svc_name* **[log] uplink { tcp | udp } { { *source_address source_wildcard* | **any** | *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port* | **range** *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port* | **range** *start_dest_port end_dest_port*] }**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.
svc_name must be a string of 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to an integer value from 0 to 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

range *start_source_port end_source_port*

Specifies that all source TCP ports within a specific range are to be filtered.
start_source_port is the initial port in the range and *end_source_port* is the final port in the range.
Both *start_source_port* and *end_source_port* can be configured to an integer value from 0 to 65535.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. *dest_port* must be configured to an integer value from 0 to 65535.

range *start_dest_port end_dest_port*

Specifies that all destination TCP ports within a specific range are to be filtered. *start_dest_port* is the initial port in the range and *end_dest_port* is the final port in the range. Both *start_dest_port* and *end_dest_port* can be configured to an integer value from 0 to 65535.

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and UDP packets coming from any host are matched:

```
redirect css service chgsvc1 uplink udp any
```

The following sets the insertion point to before the rule definition above:

```
before redirect css service chgsvc1 uplink udp any
```

The following command sets the insertion point after the rule definition above:

```
after redirect css service chgsvc1 uplink udp any
```

The following deletes the rule definition above:

```
no redirect css service chgsvc1 uplink udp any
```

redirect nexthop (by IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log]** *source_address source_wildcard*

after redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log]** *source_address source_wildcard*

before redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log]** *source_address source_wildcard*

no redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log]** *source_address source_wildcard*

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The IP address to which the IP packets are redirected.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alpha and/or numeric string from 1 to 79 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

Usage

Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of redirect rules as it does not require a rule for each source and destination pair.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at *192.168.10.4*, the context with the context ID of *23* and the source IP and wildcard of *198.162.22.0* and *0.0.0.31*:

```
redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following sets the insertion point to before the first rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following command sets the insertion point after the second rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

redirect nexthop (any)

Used to redirect subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**

after redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**

before redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**

no redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The IP address to which the IP packets are redirected.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alpha and/or numeric string from 1 to 79 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage

Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

Important: It is suggested that any rule which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at *192.168.10.4*, the context with the context ID of *23* and any source IP:

```
redirect nexthop 192.168.10.4 context 23 any
```

The following sets the insertion point to before the first rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 any
```

The following command sets the insertion point after the second rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 any
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 any
```

redirect nexthop (by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] host** *source_ip_address*

after redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] host** *source_ip_address*

before redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] host** *source_ip_address*

no redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] host** *source_ip_address*

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The IP address to which the IP packets are redirected.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alpha and/or numeric string from 1 to 79 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

Usage

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at *192.168.10.4*, the context with the context ID of *23* and a host IP address of *192.168.200.11*:

```
redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following sets the insertion point to before the first rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following command sets the insertion point after the second rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

redirect nexthop (by source ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] icmp { ***source_address source_wildcard* **| any | host** *source_host_address* **} { ***dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

after redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] icmp { ***source_address source_wildcard* **| any | host** *source_host_address* **} { ***dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

before redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] icmp { ***source_address source_wildcard* **| any | host** *source_host_address* **} { ***dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

no redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] icmp { ***source_address source_wildcard* **| any | host** *source_host_address* **} { ***dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The IP address to which the IP packets are redirected.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alpha and/or numeric string from 1 to 79 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value from 0 through 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value from 0 through 255.

Usage

Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk. The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at *fe80::c0a8:a04*, the context with the context ID of *23*, and ICMP packets coming from the host with the IP address *2002::c6a2:64195*:

```
redirect nexthop fe80::c0a8:a04 context 23 icmp host 2002::c6a2:6419
```

The following sets the insertion point to before the first rule defined above:

```
before redirect nexthop fe80::c0a8:a04 context 23 icmp host
2002::c6a2:6419
```

The following command sets the insertion point after the second rule defined above:

```
after redirect nexthop fe80::c0a8:a04 context 23 icmp host
2002::c6a2:6419
```

The following deletes the first rule defined above:

```
no redirect nexthop fe80::c0a8:a04 context 23 icmp host 2002::c6a2:6419
```

redirect nexthop (by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] ip {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The IP address to which the IP packets are redirected.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 through 79 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.

- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

protocol *num*

Indicates that the packet filtering is to be applied to a specific protocol number.
num can be an integer from 0 through 255.

Usage

Block IP packets when the source and destination are of interest.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

redirect nexthop (by TCP/UDP packets)

Used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] { tcp | udp } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port*] }**

after redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] { tcp | udp } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port*] }**

before redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] { tcp | udp } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port*] }**

no redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] { tcp | udp } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port*] }**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The IP address to which the IP packets are redirected.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 through 79 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TCP packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to an integer value from 0 to 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to an integer value from 0 to 65535.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at *fe80::c0a8:a04*, the context with the context ID of *23*, and UDP packets coming from any host are matched:

```
redirect nexthop fe80::c0a8:a04 context 23 udp any
```

The following sets the insertion point to before the rule defined above:

```
before redirect nexthop fe80::c0a8:a04 context 23 udp any
```

The following command sets the insertion point after the rule defined above:

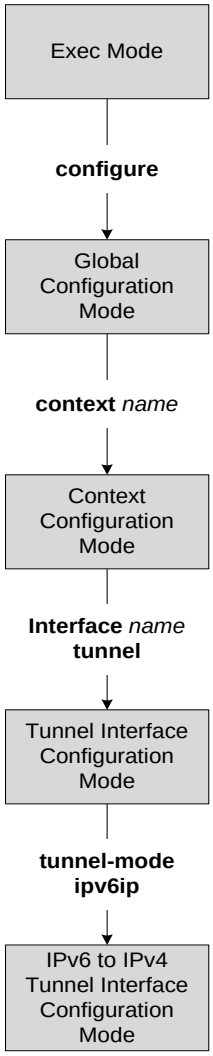
```
after redirect nexthop fe80::c0a8:a04 context 23 udp any
```

The following command deletes the first rule defined above:

```
no redirect nexthop fe80::c0a8:a04 context 23 udp any
```

Chapter 162
IPv6 to IPv4 Tunnel Interface Configuration Mode Commands

The IPv6 to IPv4 Tunnel Interface Configuration Mode is used to create and manage the IP interfaces for addresses, address resolution options, etc.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

destination address

Configures the destination of the tunnelled packets for a manual tunnel.

Product

All

Privilege

Administrator

Syntax

```
destination address address
no destination address
```

no

Removes configuration for the specified keyword.

address

Specifies the IP address of the destination device. *address* must be specified in IPv4 dotted decimal or IPv6 colon-separated notation.

Usage

Use this command to configure the IP address of the destination end of the tunnel.

Example

The following command sets the destination address for packets on this tunnelled interface to *10.2.3.4*:

```
destination address 10.2.3.4
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

mode

Configures the mode of IPv6 to IPv4 tunneling. The default is set to manual mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
mode { 6to4 | manual }
default mode
```

6to4

Configures automatic IPv6-to-IPv4 (6to4) tunnels as specified in RFC 3056.

manual

Configures point-to-point manual IPv6-to-IPv4 tunnels by specifying the IPv4 address of the tunnel remote end.

default

Resets the mode of IPv6-to-IPv4 tunneling to manual mode.

Usage

There can be only one IPv6-to-IPv4 tunnel possible in a context. Once an IPv6-to-IPv4 tunnel is configured, all subsequent tunnels will be configured as manual tunnels.

Example

The following command configures the mode to IPv6-to-IPv4 (*6to4*).

```
mode 6to4
```

The following command configures the mode to *6to4*.

```
mode manual
```

source

Configures the source of tunneled packets.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

source { address *ip_address* **| interface***interface_name***}**

no source { address | interface }

address *ip_address*

Specifies the IPv4 address to use as the source address of the tunnel.

ip_address must be expressed in IPv4 dotted-decimal notation.

interface *interface_name*

Specifies the name of a non-tunnel IPv4 interface, whose address is used as the source address of the tunnel. *interface* must be an alphanumeric string of 1 through 79 characters.

no source { address | interface }

Removes configuration for the specified keyword.

Usage

Configures the source IPv4 address of the tunnel by either specifying the IP address (host address) or by specifying another configured non-tunnel IPv4 interface. The source address must be an existing interface address before it is used. State of source address will affect the operational state of the tunnel.

Example

The following command configures the source address of the tunnel.

```
source address 10.2.3.4
```

The following command specifies the source interface as *testsource1*.

```
source interface testsource1
```

tos

Configures the type of service (TOS) settings of the outer IPv4 header of the tunneled packets.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

tos { copy | value *tos_value* **}**

default tos

copy

Copies the DC octet of the IPv6 packet to the TOS octet of IPv4 packet.

default

Configures default setting for the specified keyword.

value *tos_value*

Configures the raw TOS value ranging from 0 to 255. The default is 0.

Usage

Sets the TOS parameter to be used in the tunnel transport protocol or copies the TOS value from the original IPv6 DC byte to the TOS value of the encapsulating IPv4 header.

Example

The following command sets the tos value to *1*:

```
tos value 1
```

ttl

Configures the TTL (Time to live) value of the outer IPv4 header of the tunneled packets.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

ttl value *ttl_value*

default

Configures default setting for the specified keyword.

value *ttl_value*

ttl_value is an integer from 1 through 255. The default is 16.

Usage

Configures the TTL parameter to be used in the tunnel transport protocol.

Example

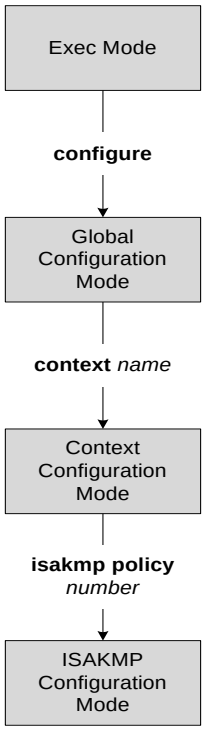
The following command sets the TTL value to *25*.

```
ttl value 25
```

Chapter 163
ISAKMP Configuration Mode Commands

The ISAKMP Configuration Mode is used to configure Internet Security Association Key Management Protocol (ISAKMP) policies that are used to define Internet Key Exchange (IKE) security associations (SAs).

Modification(s) to an existing ISAKMP policy configuration will not take effect until the related security association has been cleared. Refer to the **`clear crypto security-association`** command described in the *Exec Mode (A–C) Commands* chapter for more information.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

authentication

Configures the ISAKMP policy authentication mode.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
authentication preshared-key

[ default | no ] authentication
```

default authentication

Restores the default setting of this parameter. This command is enabled by default.

no authentication

Disables the preshared key authentication mode.

preshared-key

Specifies that the policy will be authenticated through the use of the pre-shared key.

Usage

When the system is configured to use ISAKMP-type crypto maps for establishing IPSec tunnels, this command is used to indicate that the policy will be authenticated through the use of the pre-shared key configured in the ISAKMP crypto map.

Example

The following command sets policy authentication mode to use a pre-shared key:

```
authentication preshared-key
```

encryption

Configures the encryption protocol to use to protect subsequent IKE SA negotiations.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
encryption { 3des-cbc | aes-cbc-128 | aes-cbc-256 | des-cbc }

[ default | no ] encryption
```

default encryption

Restores the default setting of this parameter.

no encryption

Removes a previously configured encryption type.

3des-cbc

Specifies that the encryption protocol is Triple Data Encryption Standard (3DES) in chain block (CBC) mode.

aes-cbc-128

Specifies that the encryption protocol is Advanced Encryption Standard (AES) in CBC mode with a 128-bit key.

aes-cbc-256

Specifies that the encryption protocol is Advanced Encryption Standard (AES) in CBC mode with a 256-bit key.

des-cbc

Specifies that the encryption protocol is DES in CBC mode. This is the default setting.

Usage

Once the D-H exchange between the system and the security gateway has been successfully completed, subsequent IKE SA negotiations will be protected using the protocol specified by this command.

Example

The following command sets the IKE encryption method to 3des-cbc:

```
encryption 3des-cbc
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

group

Configures the Oakely group (also known as the Diffie-Hellman [D-H] group) in which the D-H exchange occurs.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
group { 1 | 2 | 5 }

[ default | no ] group
```

default group

Restores the default setting of this parameter.

no group

Removes a previously configured group.

{ 1 | 2 | 5 }

Default: **1**

Specifies the number of the Oakley group. The following groups are allowed:

- **1**: Enables Oakley Group 1 using a 768-bit modp as defined in RFC 2409.
- **2**: Enables Oakley Group 2, using a 1024-bit modp as defined in RFC 2409.
- **5**: Enables Oakley Group 5, using a 1536-bit modp as defined in RFC 3526.

Usage

Specifies the Oakley group that determine the length of the base prime numbers that are used during the key exchange process.

Example

The following command sets the group to *5* which specifies 1536-bit base prime numbers:

```
group 5
```

hash

Configures the IKE hash protocol to use during IKE SA negotiations.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator\

Syntax

```
hash { md5 | sha1 }

[ default | no ] hash
```

default

Restores the default setting of this parameter.

no

Removes a previously configured hash algorithm.

md5

Specifies that the hash protocol is Message Digest 5 truncated to 96 bits.

sha1

Specifies that the hash protocol is Secure Hash Algorithm-1 truncated to 96 bits. This is the default setting for this command.

Usage

Use this command to configure the hash algorithm used during key negotiation.

Example

Set the hash algorithm to Message-Digest 5 by entering the following command:

```
hash md5
```

lifetime

Configures the lifetime of the IKE Security Association (SA).

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

lifetime *seconds*

default lifetime

default lifetime

Restores the default setting of this parameter.

seconds

Default: 86400
The number of seconds for the SA to live. *seconds* must be an integer from 60 to 86400.

Usage

Use this command to set the time that an ISAKMP SA will be valid. The lifetime is negotiated with the peer and the lowest configured lifetime duration is used.

Example

The following command sets the SA lifetime to 100 seconds:

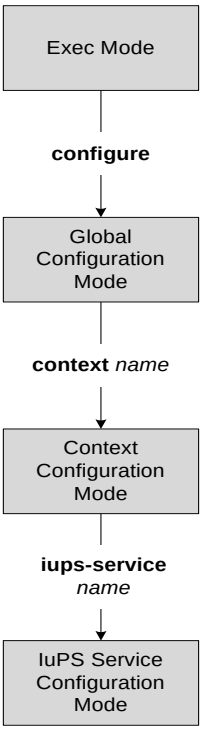
```
lifetime 100
```

Chapter 164
IuPS Service Configuration Mode Commands

The IuPS Service configuration mode is used to define properties for the IuPS service which controls the Iu-PS interface connections to Radio Network Controllers (RNCs) of the UMTS Terrestrial Radio Access Network (UTRAN).

In this mode, the prompt will appear similar to:

```
[<context_name>]hostname(config-ctx-iups-service)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

access-protocol

This command configures the access protocol parameters for the IuPS service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

access-protocol sccp-network *sccp_net_id*

no access-protocol sccp-network

no

Removes a previously configured access protocol value.

sccp-network *sccp_net_id*

Specifies the Signaling Connection Control Part (SCCP) for this IuPS service to use.
sccp_net_id must be an integer from 1 to 16.

Usage

Use this command to configure access protocol parameters for the current IuPS service.

Example

The following command specifies that the current Iu-PS service should use SCCP *1*:

```
access-protocol sccp-network 1
```

blacklist-timeout-gtpu-bind-addresses

This command specifies the time period that a GTP-U bind address (loopback address) will not be used (is blacklisted) in RAB-Assignment requests after a RAB assignment request, with that GTP-U bind address, has been rejected by an RNC with the cause - Unspecified Error. This is a failure at the RNC's GTP-U IP interface.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

blacklist-timeout-gtpu-bind-addresses *seconds*

default blacklist-timeout-gtpu-bind-addresses

default

Resets the blacklist time to 60 seconds.

seconds

Number of seconds that the GTP-U bind (loopback) address will not be used in a RAB-Assignment request. *seconds* : Must be an integer from 1 to 1800.

Usage

Use this command to configure the blacklist period.

Example

The following command specifies a 15 minutes (*460 seconds*) blacklist period.

```
blacklist-timeout-gtpu-bind-addresses 460
```

empty-cr

This command allows the operator to determine how empty Connection Request messages will be handled.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
empty-cr procedure reject

[ default | no ] empty-cr procedure reject
```

default | no

Using either **default** or **no** with the command disables the rejection function and returns the system to the default behavior, which is to ignore receipt of the empty CRs.

Usage

Use this command to enable/disable the procedure for handling empty (not containing dataparameters) Connection Request (CR) messages.
This feature can be used in the following scenario: During 4G to 3G handovers, some Connection Requests from mobile subscribers might be ignored by the SGSN, even though their UE would display that the WCDMA was available. The RNC would send an SCCP Connection Request (CR) over the Iu interface to the SGSN. Normally, this message contains a RANAP message and GMM, but according to 3GPP and ITU Q.713 standards, it is permissible to send an SCCP CR without any data parameters. In such a situation, normally the SGSN would ignore these SCCP CR messages, because without these data parameters the SGSN would be unable to derive the DeMux key which is the basis for determining the Session Manager instance to be used for a subscriber. Using this feature allows the SGSN to send a Reject to the mobile subscriber when an "empty" SCCP CR is sent from their UE.
Fields have been added to the output of the following CLI show commands to track the receipt and rejection of Connect Request (CR) messages:

- show gmm-sm statistics
- show gmm-sm statistics verbose

Example

The following command enables the empty CR handling procedure:

```
empty-cr procedure reject
```

The following command disables the empty CR handling procedure:

```
default empty-cr procedure reject
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Return to the Exec mode.

exit

Exits the current configuration mode and returns to the previous configuration mode, the context configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the context configuration mode.

force-authenticate consecutive-security-failure

Disable/enable authentication when the MS/UE security fails and configures the procedures and frequency for authentication

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Syntax

force-authenticate consecutive-security-failure { inter-sgsn-rau | local-messages count *frequency* **| non-local-messages count** *frequency* **}**

[default | no] force-authenticate consecutive-security-failure { inter-sgsn-rau | local-messages | non-local-messages }

default

Resets the values to defaults. Forced authentication is enabled for all the types of event procedures with the default values for determining frequency for authentication.

no

Disables the specified authentication configuration.

inter-sgsn-rau

Default: enabled
Enables/disables authentication for inter-SGSN RAU.
The SGSN does not remember previous inter-SGSN-RAU failures for a P-TMSI/RAI because the SGSN clears all contexts on the occurrence of an inter-SGSN-RAU security failure. So the next inter-SGSN-RAU can only be authenticated forcefully if it comes before the previous context is cleared. This type of forced authentication is enabled by default because this type of failure is fairly common.

local-messages count *frequency*

Default: 5
Enables/ disables authentication for local messages (such as local RAUs, Service Requests, Detach Requests, etc) . Consecutive security failures is fairly rare for local messages so the default count frequency is fairly high, 5. Setting the count frequency enables the feature and sets the number of consecurity local message security failures that must occur prior t o authentication being forced.
frequency: Enter an integer from 1 to 10.

non-local-messages count *count*

Default: 1
Enables/ disables authentication for non-local messages (such as inter-RAT RAUs and all types of attaches) . Consecutive security failures for non-local messages is fairly common so the default count frequency is 1. Setting the count frequency enables the feature and sets the number of consecurity non-local message security failures that must occur prior t o authentication being forced.
frequency: Enter an integer from 1 to 10.

Usage

GMM authentication is optional for UMTS. When GMM authentication is skipped, the SGSN and the MS continue to re-use the latest keys exchanged during the most recent GMM authentication procedure. This can result in the SGSN and the MS going out of sync with the CK and IK currently in use. If a mismatch occurs when the MS continues to use the correct parameters (e.g., cksn or P-TMSI signature) in the next Iu and if the SGSN skips authentication on the Iu, then, usually, the security mode will timeout or be rejected because the MS will not be able to decipher or perform an integrity check on the network messages. This scenario results in a lot of useless signaling in the network. This command allows the operator to enable a forced GMM authentication that will either resolve this type of problem or avoid it. As well, the operator can configure a frequency of authentication that best meets their needs.

Example

The following command enables forced authentication after every *3rd* local message security failure:

```
force-authenticate consecutive-security-failure local-messages count 3
```

gtpu

This commands configures parameters for the GTP user (GTP-U) dataplane.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gtpu { bind *ip_addr* **| echo-interval** *seconds* **| max-retransmissions** *number* **| retransmission-timeout** *seconds* **}**

no gtpu { bind address *ip_addr* **| echo-interval | max-retransmissions | retransmission-timeout }**

default gtpu { echo-interval | max-retransmissions | retransmission-timeout }

no

Removes the configured parameter value.

default

Sets the specified parameter to its default setting.

bind address *ip_addr*

This command binds the specified IP address to the Iu-PS GTP-U endpoint.
ip_addr: Must be an IP v4 IP address in dotted decimal notation.

echo-interval *seconds*

Default: 60
Configures the rate, in seconds, at which GTP-U echo packets are sent to the UTRAN over the Iu-PS interface.
seconds : Must be an integer from 60 through 3600.

max-retransmissions *number*

Default: 5
Configures the maximum number of transmission retries for GTP-U packets.
number : Must be an integer from 0 through 15.

retransmission-timeout *seconds*

Default: 5
Configures the retransmission timeout for GTPU packets in seconds.
seconds : Must be an integer from 1 through 20.

Usage

Use this command to configure GTP-U parameters for the Iu-PS interface.

Example

The following command binds the IP address *192.168.0.10* to the Iu-PS interface for communication with the UTRAN:

```
gtpu bind address 192.168.0.10
```

iu-hold-connection

Defines the type and duration of the Iu hold connection.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

iu-hold-connection { always [hold-time *time* **] | requested-by-ms [hold-time** *time* **] }**

default iu-hold-connection

no iu-hold-connection

default

Resets the Iu hold connection parameters to requested-by-ms and 100 second duration.

no

Removes the configuration information for the specified Iu hold connection parameter.

always

Specifies that there is always to be an Iu hold connection procedure.

requested-by-ms

Specifies that there is only an Iu hold connection procedure if requested by the MS/UE.
This is the default setting for Iu-hold-connection.

hold-time *time*

This variable configures the interval (in seconds) that the SGSN holds the Iu connection.
time: must be an integer from 10 to 3600.
Default is 100.

Usage

Define the amount of time the Iu connection will be held open.

Example

Instruct the SGSN to hold the Iu connection open for 120 seconds

```
iu-hold-connection always hold-time 120
```

iu-recovery

This command enables the Iu recovery function.

Important: This command has been deprecated and is no longer available in most 12.0 or 12.2 releases.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
iu-recovery

no iu-recovery
```

no

Disables IU recovery.

Usage

Enable or disable Iu recovery function that should be used whenever sessions are recovered.

Example

The following command disables the Iu Recovery function:

```
no iu-recovery
```

iu-release-complete-timeout

Configures the SGSN's timer for waiting for an Iu Release Complete message from the RNC.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

iu-release-complete-timeout *time*

default iu-release-complete-timeout

default

Resets the timer to its default setting.

time

This variable defines the amount of time (in seconds) that the SGSN waits to receive an 'Iu Release Complete' message from the RNC.
Default: 10.
time: Must be an integer from 1 to 60.

Usage

Configure the number of seconds that the SGSN waits to receive the Iu Release Complete message.

Example

Set the SGSN to wait 20 seconds for Iu-Release-Complete:

```
iu-release-complete-timeout 20
```

loss-of-radio-coverage ranap-cause

This command sets the detection cause included in the Iu Release message. This command is unique to releases 9.0 and higher.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

loss-or-radio-coverage ranap-cause *cause_number*

default loss-of-radio-coverage ranap-cause

default

This keyword resets the configuration to the default cause ID number.

ranap-cause *cause_number*

This number identifies the reason the SGSN has detected, from Iu Release messages, for the loss of radio coverage (LORC). This value is included in the IE messages the SGSN sends to either the GGSN or the GGSN and the peer SGSN to indicate LORC state. The range of reasons is a part of the set defined by 3GPP 25413.
cause_number : Must be an integer from 1 to 512.
Default: 46 (MS/UE radio connection lost)

Usage

By defining a cause code, the SGSN knows to detect the LORC state of the mobile from Iu Release messages it receives for the subscriber. This configuration also instructs the SGSN to include the defined cause code for the LORC state in the IE portion of various messages sent to the GGSN and optionally the peer SGSN.
This command is one of the two commands required to enable the SGSN to work with the GGSN and, optionally the peer SGSN, to implement the Overcharging Protection feature (see the *SGSN Overview* in the *SGSN Administration Guide* for feature details. The other command needed to implement the Overcharging Protection feature is the **gtp private extension** command explained in the *SGSN APN Policy Configuration Mode* chapter of the *Command Line Interface Reference*.

Example

Use the following command to set the cause code to indicate that there are no radio resources available in the target cell, cause *53*.

loss-or-radio-coverage ranap-cause 53

mbms

This command is in development for future use so the command and keywords that you might see are **not** currently supported.

Product

SGSN

network-sharing cs-ps-coordination

Enables/disables the SGSN service to perform a CS-PS coordination check.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
network-sharing cs-ps-coordination

default network-sharing cs-ps-coordination

no network-sharing cs-ps-coordination
```

default

Including this keyword resets the SGSN service to allow the check to be performed.

no

Disables this feature for the SGSN service.

Usage

Use this command to facilitate the network sharing functionality. With this command, the SGSN can be instructed to perform a check to determine if CS-PS coordination is needed.
3GPP TS 25.231 section 4.2.5 describes the functionality of the SGSN to handle CS-PS (circuit-switching/packet-switching) coordination for attached networks not having a Gs-interface. In compliance with the standard, the SGSN rejects an Attach in a MOCN configuration with cause 'CS-PS coordination required', after learning the IMSI, to facilitate the RNC choosing the same operator for both CS and PS domains.

Example

Use the following syntax to disable the CS-PS coordination check:

```
no network-sharing cs-ps-coordination
```

network-sharing failure-code

Configure the reject cause code to included in network-sharing Reject messages.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

network-sharing failure *failure_code*

default network-sharing failure

default

Resets the SGSN service to use the default cause code,14 (GPRS services not allowed in this PLMN).

failure_code

Enter one of the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message

- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

Usage

Use this command to determine which failure code will be included in Reject messages sent by the SGSN when there is a network-sharing failure.

Example

Use the following syntax to indicate that roaming is not allowed (*#13*) as the cause for the network-sharing failure:

```
network-sharing failure 13
```

plmn

Configures the PLMN (public land mobile network) related parameters for the IuPS service. This command is appicable to releases 8.1 and higher.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

plmn id mcc *mcc_num* **mnc** *mnc_num* **[network-sharing common-plmn mcc** *mcc_num* **mnc** *mnc_num* **[plmn-list mcc** *mcc_num* **mnc** *mnc_num* **[mcc** *mcc_num* **mnc** *mnc_num***+]]]**

no plmn id

no

Removes the PLMN ID from the configuration.

id

Creates a PLMN configuration instance based on the PLMN ID (comprised of the MCC and MNC). In accordance with TS 25.413, the SGSN supports up to 32 PLMN configurations for shared networks.

mcc *mcc_num*

Specifies the mobile country code (MCC) portion of the PLMN's identifier.
mcc_num: The PLMN MCC identifier and can be configured to any integer value between 100 and 999.

mnc *mnc_num*

Specifies the mobile network code (MNC) portion of the PLMN's identifier.
mnc_num: The PLMN MNC identifier and can be configured to any 2-digit or 3-digit value between 00 and 999.

network-sharing common-plmn mcc *mcc_num* **mnc** *mnc_num*

When network sharing is employed, this set of keywords is required to define the PLMN ID of the common PLMN. The common PLMN is usually not the same as the local PLMN.

plmn-list mcc *mcc_num* **mnc** *mnc_num*

When network sharing is employed and more than two PLMNs are available, then use the **plmn-list** keyword to begin a list of all additional PLMNs.

Usage

Use this command to configure the PLMN associated with the SGSN. There can only be one PLMN associated with an SGSN unless one of the following features is enabled and configured: network sharing or multiple PLMN.
For network sharing, use of the **network-sharing** keywords make it possible to identify more than one PLMN. Including the PLMN identified initially. None have precedence. They are all treated equally but they

must each be unique. In a MOCN configuration, the PLMN list will not be used as there would only be one local PLMN.
For multiple PLMN support, the SGSN can support up to 8 Iu-PS configurations for PLMNs. These Iu-PS service configurations must be associated with the SGSN via the **ran-protocol** command in the SGSN Service configuration mode.

Example

Use the following command to identify a PLMN by the MCC *313* and MNC *23* and instruct the SGSN to perform network sharing with a single *common PLMN* identified by MCC *404* and MNC *123*:

```
plmn id mcc 313 mnc 23 network-sharing common-plmn mcc 404 mnc 123
```

rab-assignment-response-timeout

Configures the RAB assignment timer.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

rab-assignment-response-timeout *time*

default rab-assignment-response-timeout

default

Resets the timer to its default setting.

time

This variable configures the amount of time (in seconds) that the SGSN waits to receive a RAB assignment from the RNC.
time: must be an integer from 1 to 60.
Default: 8.

Usage

This command defines time the SGSN waits for the completion of the RAB assignment procedure.

Example

Change the timer setting to *11* seconds.

rab-assignment-response-timeout 11

radio-network-controller

This command creates an instance of an RNC configuration to associate with the IuPS service for the SGSN. This command is only available in release 8.0; use the **rnc** command for releases 8.1 and higher.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

radio-network-controller id *rnc_id* **mcc** *mcc_num* **mnc** *mnc_num*

no radio-network-controller id *rnc_id* **mcc** *mcc_num* **mnc** *mnc_num*

no

Removes the configuration information for the specified RNC.

id *rnc_id*

Define the instance number of the RNC configuration.
rnc_id : Must be an integer from 0 to 4095.

mcc *mcc_num*

Specifies the mobile country code (MCC).
mcc_num : Must be an integer between 100 and 999.

mnc *mnc_num*

Specifies the mobile network code (MNC).
mnc_num : Must be an integer between 00 and 999.

Usage

Use this command to configure information for the IuPS service to use to contact specific RNCs.
This command also provides access to the RNC configuration mode.

Example

The following command creates or accesses RNC configuration instance *#1* with MCC of *131* and MNC of *22*:

```
radio-network-controller id 1 mcc 131 mnc 22
```

relocation-alloc-timeout

This command defines the amount of time the SGSN waits for a Relocation Request message.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

relocation-alloc-timeout *timeout_value*

default relocation-alloc-timeout

default

Resets the configuration to a 5 second wait time.

timeout_value

Time in seconds that the SGSN waits to receive a Relocation Request message.
timeout_value : Must be an integer from 1 to 60.
Default : 5 seconds.

Usage

Use this command to configure the number of seconds the SGSN will wait for a Relocation Request message to be received. This timeout needs to be set with sufficient time so that SRNS procedure aborts can be avoided if the peer fails to respond in a timely fashion in the case of a hard handoff.

Example

The following command sets the wait time to *10* seconds.

```
relocation-alloc-timeout 10
```

relocation-complete-timeout

This command specifies the maximum time for the SGSN to wait for a Relocation Completion from the core network.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

relocation-complete-timeout *timeout_value*

default relocation-complete-timeout

default

Resets the configuration to a 5 second wait time.

timeout_value

Time in seconds that the SGSN waits for relocation to be completed.
timeout_value : Must be an integer from 1 to 60.
Default : 5 seconds.

Usage

Use this command to configure the number of seconds the SGSN will wait for a relocation to be completed. This timeout needs to be set with sufficient time so that SRNS procedure aborts can be avoided if the peer fails to respond in a timely fashion in the case of a hard handoff.

Example

The following command sets the wait time for *10* seconds.

```
relocation-complete-timeout 10
```

reset

Defines the configuration specific to the RESET procedure.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
reset { ack-timeout time | guard-timeout time | max-retransmissions retries | sgsn-initiated }

default reset { ack-timeout | guard-timeout | max-retransmissions | sgsn-initiated }

no reset sgsn-initiated
```

default

Returns to the default settings for the Reset procedure.

no

Removes the SGSN-initiated reset procedure from the configuration.

ack-timeout *time*

Configures the interval (in seconds) for which the SGSN waits for RESET-ACK from the RNC.
time must be an integer from 5 to 60.
Default: 20.

guard-timeout

Configures the interval (in seconds) after which the SGSN sends RESET-ACK to the RNC.
time must be an integer from 5 to 60.
Default : 10

max-retransmissions

Configures maximum retries for RESET message.
retries must be an integer from 0 to 2.
Default: 1.

sgsn-initiated

Enables SGSN initiated RESET procedure.
Default: disabled.

Usage

Configures the parameters that determine a RESET.

Example

Use the following to have the SGSN initiate the RESET procedure:

```
reset sgsn-initiated
```

rnc

This command creates or accesses an instance of an RNC (radio network controller) configuration.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

rnc id *rnc_id*

no rnc id *rnc_id*

no

Removes the configuration information for the specified RNC.

id *rnc_id*

Set the identification number of the RNC configuration instance.
rnc_id : Must be an integer from 0 to 4095 for 8.1 releases. Must be an integer from 0 to 65535 for releases 9.0 and higher.

Usage

Use this command to configure information for the IuPS service to use to contact specific RNCs.
This command also provides access to the RNC configuration mode.

Example

The following command creates an RNC configuration instance *#3442*:

```
rnc id 3442
```

security-mode-complete-timeout

This command configures the security mode timer.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

security-mode-complete-timeout *time*

default security-mode-complete-timeout

default

Resets the timer configuration to the default settings.

time

Configures the interval (in seconds) the SGSN waits for the security mode from the MS to complete.
time must be an integer from 1 to 60.
Default is 5

Usage

Use this command to configure the timer that determines how long the SGSN waits for a Security Mode Complete message from the MS (mobile station).

Example

Instruct the SGSN to wait 7 seconds:

```
security-mode-complete-timeout 7
```

srns-context-response-timeout

This command configures the SGSN context response timer.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

srns-context-response-timeout *time*

default srns-context-response-timeout

default

Resets the timer configuration to the default setting.

time

Configures the interval (in seconds) for which the SGSN waits for an SRNS Context Request message.
time must be an integer from 1 to 60.
Default: 5.

Usage

Configures the time to wait before the SGSN sends a response to the SRNS Context-Request message.

Example

Configure the SGSN to wait 7 seconds for an SRNS Context-Request response:

```
srns-context-response-timeout 7
```

tigoc-timeout

This command configures the TigOc interval.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

tigoc-timeout *time*

default tigoc-timeout

default

Resets the timer configuration to the default setting.

time

This command sets the time in seconds.
time : Must be an integer from 1 to 60.
Default: 5.

Usage

Define the amount of time that the SGSN ignores any overload messages for TigOc interval after receiving one overload message from the RNC.

Example

Use the following command to change the default TigOc interval to *4* seconds:

```
tigoc-timeout 4
```

tintc-timeout

This command configures the TinTc interval..

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

tintc-timeout *time*

default tintc-timeout

default

Resets the timer configuration to the default setting.

time

Set the number of seconds to wait.
time : Must be an integer from 1 to 60.
Default: 30.

Usage

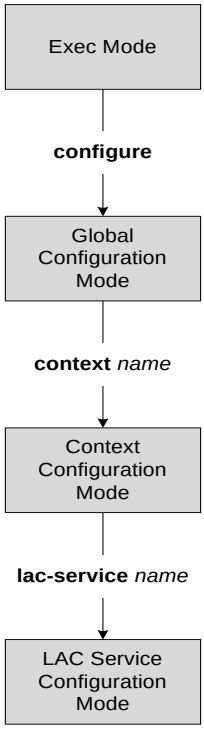
Define *4* as the number of seconds that the SGSN waits before decrementing (by one) the traffic level of the RNC.

Example

```
tintc-timeout 4
```

Chapter 165
LAC Service Configuration Mode Commands

The LAC Service Configuration Mode is used to create and manage L2TP services within contexts on the system. L2TP Access Concentrator (LAC) services facilitate tunneling to peer L2TP Network Servers (LNSs).



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

allow

This command configure the system to allow different attributes in the LAC Hostname Attribute Value Pair (AVP) and Called-Number AVP for L2TP messages exchanged between LAC and LNS.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
allow {aaa-assigned-hostname | called-number value apn}

[ no | defualt ] allow {aaa-assigned-hostname | called-number value apn}
```

no

Disable the configured attribute and returns to the behavior that uses the LAC-Service name as the HostName AVP.

aaa-assigned-hostname

When enabled if AAA assigns a valid Tunnel-Client-Auth-ID attribute for the tunnel, it is used as the HostName AVP in the L2TP tunnel setup message.
This keyword works in conjunction with the **local-hostname** *hostname* keyword applied via the **tunnel l2tp** command in APN Configuration mode.
When Tunnel parameters are not received from the RADIUS Server, Tunnel parameters configured in an APN are considered for the LNS peer selection. When APN configuration is selected, the local-hostname configured with the **tunnel l2tp** command in the APN for the LNS peer will be used as an LAC Hostname.

called-number value apn

Configures the system to send the APN name in the Called-Number AVP as a part of ICRQ message sent to the LNS. If this keyword is not configured, Called-Number AVP will not be included in ICRQ message sent to the LNS.

Usage

Use this command to configure the attribute for the HostName AVP for L2TP messages exchanged between LAC and LNS.
LAC Hostname will be different for the subscribers corresponding to the different corporate APNs. In the absence of a AAA assigned HostName, the LAC-Service name is used as HostName. By default the LAC-Service name is used as the HostName AVP.

Example

The following command enables the use of the value of Tunnel-Client-Auth-ID attribute for the HostName AVP:

```
allow aaa-assigned-hostname
```

Use the following command to reset the behavior so that the LAC-Service uses the LAC-Service name as the HostName AVP:

```
no allow aaa-assigned-hostname
```

bind

This command assigns a local end point address to the LAC service in the current context.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

bind *ip_address* **[max-subscribers]**

no bind *ip_address*

no

Unassign, or unbind, the local end point to the LAC service.

ip_address

This must be a valid IP address entered using IPv4 dotted-decimal notation.

max-subscribers

The maximum number of subscribers that can use the endpoint for this LAC service. Must be an integer from 1 to 2500000.

Usage

Use this command to bind a local end point IP address to the LAC service.

Example

The following command binds the local end point IP address *10.10.10.100* to the LAC service in the current context:

```
bind 10.10.10.100
```

The following command removes the binding of the local end point to the LAC service:

```
no bind
```

data sequence-number

Enables data sequence numbering for sessions that use the current LAC service. Data sequence numbering is enabled by default.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
data sequence-number

no data sequence-number
```

no

Disables data sequence numbering for sessions.

Usage

An L2TP data packet header has an optional data sequence numbers field. The data sequence number may be used to ensure ordered delivery of data packets. This command is used to re-enable or disable the use of the data sequence numbers for data packets.

Example

Use the following command to disable the use of data sequence numbering:

```
no data sequence-number
```

Use the following command to re-enable data sequence numbering:

```
data sequence-number
```

default

This command sets the specified LAC service parameter to its default value or setting.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
default {data sequence-number | hide-attributes | keepalive-interval | load-balancing |
local-receive-window | max-retransmission | max-session-per-tunnel | max-tunnel-
challenge-length | max-tunnels | proxy-lcp-authentication | retransmission-timeout-first
| retransmission-timeout-max | trap all |tunnel-authentication}
```

`data sequence-number`

Enables data sequence numbering for sessions.

`hide-attributes`

Disables hiding attributes in control messages sent from the LAC to the LNS.

`keepalive-interval`

Sets the interval for send L2TP Hello keepalive if there is no control or data transactions to the default value of 60 seconds.

`load-balancing`

Sets the load balancing algorithm to be used when many LNS peers have been configured to the default of round robin.

`local-receive-window`

Sets the window size to be used for the local side for the reliable control transport to the default of 16.

`max-retransmission`

Sets the maximum number of retransmissions to the default of 5.

`max-session-per-tunnel`

Sets the maximum number of sessions per tunnel at any point in time to the default of 512.

`max-tunnel-challenge-length`

Sets the maximum length of the tunnel challenge to the default of 16 bytes.

`max-tunnels`

Sets the maximum number of tunnels for this service to the default of 32000.

proxy-lcp-authentication

Sets sending of proxy LCP authentication parameters to the LNS to the default state of enabled.

retransmission-timeout-first

Sets the first retransmit interval to the default of 1 second.

retransmission-timeout-max

Sets the maximum retransmit interval to the default of 8 seconds.

trap all

Generates all supported SNMP traps.

tunnel-authentication

Sets tunnel authentication to the default state of enabled.

Usage

Use the default command to set LAC service parameters to their default states.

Example

Use the following command to set the keep alive interval to the default value of 60 seconds:

```
default

keepalive-interval
```

Use the following command to set the maximum number of sessions per tunnel to the default value of 512:

```
default max-session-per-tunnel
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

hide-attributes

Enables hiding certain attributes (such as proxy-auth-name and proxy-auth-rsp) in control messages sent from the LAC to the LNS. The LAC hides such attributes only if tunnel authentication is enabled between the LAC and the LNS.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
hide-attributes

no hide-attributes
```

no

Disable hiding attributes.

Usage

Use this command to hide certain attributes from control messages when tunnel authentication is enabled between the LAC and the LNS.

Example

The following command enables hiding attributes:

```
hide-attributes
```

keepalive-interval

This command specifies the amount of time to wait before sending a Hello keep alive message.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

keepalive-interval *seconds*

no keepalive-interval

no

Disables the generation of Hello keepalive messages on the tunnel.

seconds

Default: 60
The number of seconds to wait before sending a Hello keepalive message. The number can be configured to an integer from 30 to 2147483648.

Usage

Use this command to set the amount of time to wait before sending a Hello keepalive message or disable the generation of Hello keep alive messages completely. A keepalive mechanism is employed by L2TP in order to differentiate tunnel outages from extended periods of no control or data activity on a tunnel. This is accomplished by injecting Hello control messages after a specified period of time has elapsed since the last data or control message was received on a tunnel. As for any other control message, if the Hello message is not reliably delivered then the tunnel is declared down and is reset. The transport reset mechanism along with the injection of Hello messages ensures that a connectivity failure between the LNS and the LAC is detected at both ends of a tunnel.

Example

Use the following command to set the Hello keepalive message interval to *120* seconds:

```
keepalive-interval 120
```

Use the following command to disable the generation of Hello keepalive messages:

```
no keepalive-interval
```

load-balancing

Configures how LNSs are selected for this LAC service.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
load-balancing {balanced | prioritized | random}
```

balanced

LNS selection is made without regard to prioritization, but in a sequential order that balances the load across the total number of LNS nodes available.

prioritized

LNS selection is made based on the priority assigned in the Tunnel-Preference attribute. An example of this method is three LNS nodes, with preferences of 1, 2, and 3 respectively. In this example, the RADIUS server always tries the tunnel with a preference of 1 before using any of the other LNS nodes.

random

Default: Enabled
LNS selection is random in order, wherein the RADIUS server does not use the Tunnel-Preference attribute in determining which LNS to select.

Usage

Use this command to configure the load-balancing algorithm that defines how the LNS node is selected by the LAC when there are multiple peer LNSs configured in the LAC service.

Example

The following command sets the LAC service to connect to LNSs in a sequential order;

```
load-balancing balanced
```

The following command sets the LAC service to connect to LNSs according to the priority assigned through the Tunnel-Preference attribute:

```
load-balancing prioritized
```

local-receive-window

Specifies the number of control messages the remote peer LNS can send before waiting for an acknowledgement.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

local-receive-window *integer*

integer

Default: 4
Specifies the number of control messages to send before waiting for an acknowledgement. The number can be configured to an integer from 1 to 256.

Usage

Use this command to set the size of the control message receive window being offered to the remote peer LNS. The remote peer LNS may send the specified number of control messages before it must wait for an acknowledgment.

Example

The following command sets the local receive window to *10* control messages:

```
local-receive-window 10
```

max-retransmission

Sets the maximum number of retransmissions of a control message to a peer before the tunnel and all sessions within it are cleared.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

max-retransmission *integer*

integer

Default: 5
Specifies the maximum number of retransmissions of a control message to a peer. This value must be an integer from1 through 10.

Usage

Each tunnel maintains a queue of control messages to be transmitted to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval. For example; if the first retransmission occurs after 1 second, the next retransmission occurs after 2 seconds has elapsed, then the next after 4 seconds. If no peer response is detected after the number of retransmissions set by this command, the tunnel and all sessions within are cleared.
Use this command to set the maximum number of retransmissions that the LAC service sends before closing the tunnel and all sessions within. it.

Example

The following command sets the maximum number of retransmissions of a control message to a peer to *7*:

```
max-retransmissions 7
```

max-session-per-tunnel

Sets the maximum number of sessions that can be facilitated by a single a tunnel at any time.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

max-sessions-per-tunnel *integer*

integer

Default: 512
The maximum number of sessions expressed as an integer from 1 through 65535.

Usage

Use this command to set the maximum number of sessions you want to allow in a tunnel.

Example

The following command sets the maximum number of sessions in a tunnel to *5000*:

```
max-sessions-per-tunnel 5000
```

max-tunnel-challenge-length

Sets the maximum length of the tunnel challenge in bytes.The challenge is used for tunnel authentication purposes during tunnel creation.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

max-tunnel-challenge-length *bytes*

bytes

Default: 16
Specifies the maximum length (in bytes of the tunnel challenge. This must be an integer from 4 through 32.

Usage

Use this command to set the maximum length (in bytes) for the tunnel challenge that is used during tunnel creation.

Example

The following command sets the maximum length of the tunnel challenge to *32* bytes:

```
max-tunnel-challenge-length 32
```

max-tunnels

The maximum number of tunnels that the current LAC service can support.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

max-tunnels *integer*

integer

Default: 32000
The maximum number of tunnels expressed as an integer from 1 through 32000.

Usage

Use this command to set the maximum number tunnels that this LAC service can support at any on time.

Example

Use the following command to set the maximum number of tunnels for the current LAC service to *20000*:

```
max-tunnels 20000
```

peer-lns

Adds a peer LNS address for the current LAC service. Up to eight peer LNSs can be configured for each LAC service.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

peer-lns *ip_address* **[encrypted] secret** *secret* [**crypto-map** *map_name* { [**encrypted**] **isakmp-secret** *secret* }] [**description** *text*] [**preference** *integer*]

no peer-lns *ip_address*

---

no peer-lns *ip_address*

Deletes the peer LNS at the IP address specified by *ip_address*. *ip_address* must be entered in IPv4 dotted-decimal notation.

---

ip_address

The IP address of the peer LNS for the current LAC service. *ip_address* must be entered in IPv4 dotted-decimal notation.

[encrypted] secret *secret*

Designates the secret which is shared between the current LAC service and the peer LNS. *secret* must be an alphanumeric string of 1 through 256 characters that is case sensitive.
encrypted secret *secret*: Specifies that encryption should be used when communicating the secret with the peer LNS.

---

crypto-map *map_name* **{ [encrypted] isakmp-secret** *secret* **}**

map_name is the name of a crypto map that has been configured in the current context. *map_name* must be an alphanumeric string of 1 through 127 characters that is case sensitive.
isakmp-secret *secret*: The pre-shared key for IKE. *secret* must be an alphanumeric string of 1 through 127 characters that is case sensitive.
encrypted isakmp-secret *secret*: The pre-shared key for IKE. Encryption must be used when sending the key. *secret* must be an alphanumeric string of 1 through 127 characters.

---

description *text*

Specifies the descriptive text to use to describe the specified peer LNS. *text* must be an alphanumeric string of 0 through 79 characters.

---

preference *integer*

This sets the priority of the peer LNS if multiple peer LNSs are configured. *integer* must be an integer from 1 through 128.

Usage

Use this command to add a peer LNS address for the current LAC service.

Example

The following command adds a peer LNS to the current LAC service with the IP address of *10.10.10.100*, sets encryption on, specifies the shared secret to be *1b34nnf5d*, and sets the preference to *3*:

```
peer-lns 10.10.10.100 encrypted secret 1b34nnf5d preference 3
```

The following command removes the peer LNS with the IP address of *10.10.10.200* for the current LAC service:

```
no peer-lns 10.10.10.200
```

proxy-lcp-authentication

Enables and disables the sending of proxy LCP authentication parameters to the LNS.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
proxy-lcp-authentication

no proxy-lcp-authentication
```

no

Disables the sending of proxy LCP authentication parameters to the LNS.

proxy-lcp-authentication

Default: Enabled
Enables the sending of proxy LCP authentication parameters to the LNS.

Usage

Use this feature in situations where the peer LNS does not understand the proxy LCP Auth AVPs that the system sends and does not do an LCP renegotiation and tears down the call.

Example

Use the following command to disable the sending of proxy LCP authentication parameters to the LNS;

```
no proxy-lcp-authentication
```

Use the following command to re-enable the sending of proxy LCP authentication parameters to the LNS:

```
proxy-lcp-authentication
```

retransmission-timeout-first

Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted. This command sets the initial timeout for retransmission of control messages.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

retransmission-timeout-first *integer*

integer

Default: 1
The amount of time to wait (in seconds) before sending the first control message retransmission. This must be an integer from 1 through 100.

Usage

Use this command to set the initial timeout before retransmitting control messages to the peer.

Example

The following command sets the initial retransmission timeout to *3* seconds:

```
retransmission-timeout-first 3
```

retransmission-timeout-max

Configures maximum amount of time between two retransmission of control messages.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

retransmission-timeout-max *integer*

integer

Default: 8
integer is the maximum time (in seconds) to wait before retransmitting control messages expressed as e an integer from 1 through 100.

Usage

Use this command to set the maximum amount of time that can elapse before retransmitting control messages.
Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval.

Example

The following command sets the maximum retransmission time-out to *10* seconds:

```
retransmission-timeout-max 10
```

single-port-mode

This command enables/disables the L2TP LAC service always to use standard L2TP port 1701 as source port for all L2TP control and data packets originated from LAC node.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[no | default] single-port-mode
```

no

Disables the configured single source port configuration from this LAC service.

default

Default: Enabled
Sets this command to its default state of disabled. By default single source port configuration for L2TP LAC packets is disabled.

Usage

Use this command to enable or disable the single port mode for L2TP LAC service.
If this feature is enabled, then L2TP LAC service will always use standard L2TP port 1701 as source port for all L2TP control/data packets originated from LAC (instead of the default scheme in which each L2TPMgr uses a dynamic source port). L2TPMgr instance 1 will handle all L2TP calls for the service.

Caution: Changing this configuration, while the service is already running, will cause restart of the service.

Example

The following command enables the LAC service to use port 1701 as source port for all L2TP control and data packets:

```
single-port-mode
```

snoop framed-ip-address

When enabled, this feature allows the LAC to detect IP Control Protocol (IPCP) packets exchanged between the mobile node and the LNS and extract the framed-ip-address assigned to the mobile node. The address will be reported in accounting start/stop messages and displayed for subscriber sessions.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[no | default] snoop framed-ip-address
```

no

Disables the feature. Accounting start/stop will occur before the PPP session is established and the framed IP address field will be reported as 0.0.0.0.

default

Disabled.

Usage

This feature is available to address simple IP roaming scenarios. If this feature is enabled, the Accounting Start will be sent only after the framed-ip-address is detected. If the framed-ip-address is not detected within 16 seconds, an Accounting Start will be sent for the session with the 0.0.0.0 address. If the session is disconnected during the detection attempt, Accounting Start/Stop will be sent for the session. If the session renegotiates IPCP, an Accounting Stop will be generated with a framed-ip-address from the old session, and an Accounting Start will be generated with an IP address for the new session. IPv6 address detection is not supported.

Important: When this feature is enabled and the show subscribers all command is invoked, the framed-IP-address is displayed for the PDSN Simple IP subscriber in the output display.

trap

This command generates SNMP traps.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[no] trap all
```

no

Disables SNMP traps.

Usage

Use this command to enable/disable all supported SNMP traps.

Example

To enable all supported SNMP traps, enter the following command:

```
trap all
```

tunnel selection-key

Enables the creation of tunnels between an L2TP service and an LNS server on the basis of a key received from AAA server.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
tunnel selection-key { none | tunnel-client-auth-id | tunnel-server-auth-id }

default tunnel selection-key
```

default

Disables the creation of tunnel between LAC service and LNS based on a key value received from AAA server.

none

Default: Enabled
This keyword disables the creation of multiple tunnels between a pair of LAC service and LNS server. LAC will not make use of the key to choose a tunnel with LNS in this setup.

tunnel-client-auth-id

Default: Disabled
This keyword enables the creation of tunnels between LAC service and an LNS server on the basis of domain attribute “Tunnel-Client-Auth-ID” value received from AAA server.

tunnel-server-auth-id

Default: Disabled
This keyword enables the creation of tunnels between LAC service and an LNS server on the basis of domain attribute “Tunnel-Server-Auth-ID” value received from AAA server.

Usage

Use this command to enable or disable the creation of additional L2TP tunnels between LAC service and LNS server on the basis of “Tunnel-Client-Auth-ID” or “Tunnel-Server-Auth-ID” attribute value received from AAA Server in Access-Accept message. This value of attribute is treated as a key for tunnel selection and creation.
When the LAC needs to establish a new L2TP session, it first checks for an existing L2TP tunnel with the peer LNS based on the value of the key configured. If no such tunnel exists for the key, it will create a new tunnel with the LNS.
The default configuration has the selection-key as **none**. Hence, LAC will not make use of key to choose a tunnel with LNS in default setup.
The maximum number of sessions, as configured via the **max-sessions-per-tunnel** command, is applicable for each tunnel created through this command. By default, each tunnel supports 512 sessions.

If the LAC service needs to establish a new tunnel for a new L2TP session with LNS and the tunnel create request fails because maximum tunnel creation limit is reached, LAC will try other LNS addresses received from AAA server in Access-Accept message for the APN/subscriber. If all available peer-LNS are exhausted, LAC service will reject the call.

Example

The following command enables the use of "Tunnel-Server-Auth-ID" attribute value received from AAA Server in Access-Accept message as a key for tunnel selection and creation:

```
tunnel selection-key tunnel-server-auth-id
```

tunnel-authentication

Enables tunnel authentication. When tunnel authentication is enabled, a configured shared secret is used to ensure that the LAC service is communicating with an authorized peer LNS. The shared secret is configured by the **peer-lns** command in the LAC Service Configuration mode, the **tunnel l2tp** command in the Subscriber Configuration mode, or the **Tunnel-Password** attribute in the subscribers RADIUS profile.

Product

GGSN, PDSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[no] tunnel-authentication
```

no

Disables tunnel authentication.
Tunnel authentication is enabled by default.

Usage

Disable or enable the usage of secrets to authenticate a peer LNS when setting up a tunnel.

Example

To disable tunnel authentication, use the following command:

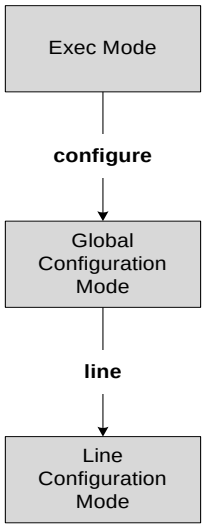
```
no tunnel-authentication
```

To re-enable tunnel authentication, use the following command:

```
tunnel-authentication
```

Chapter 166
Line Configuration Mode Commands

The Line Configuration Mode is used to manage the terminal line characteristics for output formatting.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

default

Restores the default length or width for the output to the display terminal.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
default { length | width }
```

length | width

length: restores the default value for the number of rows (length) of the output for display.
width: restores the default value for the number of columns (width) of the output for display as the number of characters.

Usage

Reset the output display properties if they had been changed during a session.

Example

```
default length

default width
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

length

Configures the output for the displays length (number of rows).

Product

All

Privilege

Security Administrator, Administrator

Syntax

length *number*

number

Specifies the number of rows (lines) of output that can be displayed at one time for the display (output) terminal. *number* must be 0 or an integer from 5 through 512, where the special value 0 implies an infinite number of rows.

Usage

Set the current session's display terminal has different display characteristics than the defaults. The special infinite value (0) is typically used when logging the output of a session from a remote machine since this will result in no pagination of output.

Example

The following commands set the length of the display to infinite and *33*, respectively.

```
length 0

length 33
```

width

Configures the output for the displays width (number of columns/characters wide).

Product

All

Privilege

Security Administrator, Administrator

Syntax

width *number*

number

Specifies the number of columns (characters) of output that can be displayed at one time for the display (output) terminal. *number* must be an integer from 5 through 512.

Usage

Set the current session's display terminal has different display characteristics than the defaults.

Example

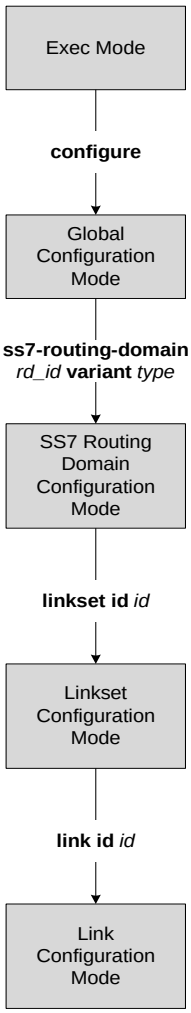
```
width 160
```

Chapter 167
Link Configuration Mode Commands

The Link configuration mode defines the MTP3 link parameters for a specific link in a linkset of an SS7 routing domain instance.

In this mode, the prompt will be similar to:

```
[local]hostname(config-ss7-rd-linkset-<#>-link-<#>)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

arbitration

This command configures link arbitration.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
arbitration { active | passive }

no arbitration
```

no

Removes the arbitration configuration for the link.

active

The SSCOP initiates the transmission of PDUs.

passive

The SSCOP waits to receive PDUs.

Usage

Sets the configuration to initiate transmission of PDUs.

Example

```
arbitration active
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

mtp2-aerm-emergency-threshold

Configure the alignment error rate monitor (AERM) emergency threshold value. This command is only available for a lowspeed-narrowband link-type.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp2-aerm-emergency-threshold *value*

default mtp2-aerm-emergency-threshold

default

Resets the parameter to the default value of 1.

value

value : Enter an integer from 1 to 50. Default: 1.

Usage

This command sets the emergency threshold for the MTP2 alignment error rate monitor.

Example

Set the emergency AERM threshold to 17:

```
mtp2-aerm-emergency-threshold 17
```

mtp2-aerm-normal-threshold

Configure the alignment error rate monitor (AERM) normal threshold value. This command is only available for a lowspeed-narrowband link-type.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp2-aerm-normal-threshold *value*

default mtp2-aerm-normal-threshold

default

Resets the parameter to the default value of 4.

value

value : Enter an integer from 4 to 100. Default: 4.

Usage

This command sets the normal threshold for the MTP2 alignment error rate monitor.

Example

Set the normal AERM threshold to 55:

mtp2-aerm-normal-threshold *55*

mtp2-eim-decrement

Configure the errored interval monitor (EIM) emergency decrement value. This command is only available for a highspeed-narrowband link-type.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp2-eim-decrement *value*

default mtp2-eim-decrement

default

Resets the parameter to the default value of 11.

value

value : Enter an integer from 1 to 63. Default: 11.

Usage

This command sets the emergency decrement value for the EIM.

Example

Reset the EIM emergency decrement to 1:

```
default mtp2-eim-decrement
```

mtp2-eim-increment

Configure the errored interval monitor (EIM) emergency increment value. This command is only available for a highspeed-narrowband link-type.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp2-eim-increment *value*

default mtp2-eim-increment

default

Resets the parameter to the default value of 198.

value

value : Enter an integer from 1 to 1023. Default: 198.

Usage

This command sets the emergency increment value for the EIM.

Example

Set the EIM emergency increment to 2:

mtp2-eim-increment *2*

mtp2-eim-threshold

Configure the errored interval monitor (EIM) emergency threshold value. This command is only available for a highspeed-narrowband link-type.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp2-eim-threshold *value*

default mtp2-eim-threshold

default

Resets the parameter to the default value of 794.

value

value : Enter an integer from 1 to 65535. Default: 794.

Usage

This command sets the emergency threshold value for the EIM.

Example

Set the EIM emergency threshold to 154:

mtp2-eim-threshold *154*

mtp2-error-correction

Configure the error correction method to be used. This command is only available for lowspeed or highspeed narrowband link-types.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
mtp2-error-correction { basic | preventive-cyclic-retransmission }

default mtp2-error-correction
```

default

Resets the parameter to the default value.

basic

Basic error correction (BEC) is a positive / negative acknowledgement method that uses backwards retransmission. This method is best for links with less than 30 ms one-way propagation delays.

preventtive-cyclic-retransmission

PCR is recommended for links with 125 ms, or higher, propagation delays.

Usage

Set the method of MTP2 layer error correct to be used on the link.

Example

Set error correction for a link with 15 ms propagaion delay::

```
mtp2-error-correction basic
```

mtp2-lssu-len

This command sets the length of the link status signal unit (LSSU) which carries link status information used to manage link alignment and indicate the status of the signaling points to each other. This command is only available for lowspeed or highspeed narrowband link-types.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp2-lssu-len *#_octets*

default mtp2-lssu-len

default

Using this keyword with the command resets the length to the default of 1 octet.

#_octets

Sets the number of octets for the length of the LSSU.
#_octets: Must be either 1 or 2.

Usage

Use this command to define the maximum amount of link status information that is to be shared between signaling points.

Example

You can use the following command to set the LSSU length to 2 octets - the maximum length:

mtp2-lssu-len *2*

mtp2-max-outstand-frames

This command sets the maximum number of outstanding packets to be sent by the link manager (linkmgr) - applicable for both high speed (HSL) and low speed (LSL) narrowband links.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp2-max-outstand-frames *#_bytes*

default mtp2-max-outstand-frames

default

Using this keyword with the command resets number of packets to the default of 7 bytes.

#_bytes

Sets the maximum number of packets sent by the linkmgr that can be allowed to be outsanding.
#_bytes: Must be an integer from 5 to 10.

Usage

The linkmgr (MTP2) sends data at a higher rate, than the narrowband (NB) E1 link speed, when in congestion and performing retransmission. This can lead to more congestion leading to more time taken for the link to come out of congestion. If using a value of 10 during congestion, then linkmgr pumps data at a rate higher than 2.5 mbps. To avoid this problem, a lower value is usually considered optimal. This configuration holds good for both HSL and LSL.

Example

Use the following command to reset the default number of outstanding packets sent by the LinkMgr:

```
default mtp2-max-outstand-frames
```

Set the maximum number of oustanding packets the linkmgr can send to 6:

```
mtp2-max-outstand-frames 6
```

mtp2-suerm-threshold

Configure the signal unit error rate monitor (SUERM) threshold. This command is only available for lowspeed-narrowband link-types.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp2-suerm-threshold *value*

default mtp2-suerm-threshold

default

Resets the parameter to the default value.

value

Defines the threshold for number of bad frames
value: Enter an integer from 64 to 1023. Default is 64.

Usage

Sets the threshold for link monitoring of bad frames.

Example

Set a new link monitoring bad frames (SEURM) threshold of 256:

mtp2-suerm-threshold *256*

mtp3-discard-priority

Configure MTP3 message discard priority.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp3-discard-priority *priority*

default mtp3-discard-priority

default

Resets the priority to the default value.

priority

priority: must be an integer between 0 and 3.
Default is 0.

Usage

Use this command to manage MTP3 messaging.

Example

mtp3-discard-priority *2*

mtp3-max-slt-try

Configure maximum number of times to retry SLT (signaling link test).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp3-max-slt-try *retries*

default mtp3-max-slt-try

default

Resets the number of retries to the default value.

retries

retries: must be an integer between 1 to 65535.
Default is 10.

Usage

Use this command to troubleshoot MTP3 link mismatch.

Example

mtp3-max-slt-try *35*

mtp3-msg-priority

Configures the priority for sending MTP3 management messages.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp3-msg-priority *priority*

default mtp3-msg-priority

default

Resets the number of priority to the default value.

priority

priority: must be an integer from 0 to 3.
Default: 0

Usage

Use this command to set the priority for sending MTP3 management messages.

Example

Use the following to set the message priority to 3:

```
mtp3-msg-priority 3
```

mtp3-msg-size

Configures the size of messages from layer 3 to layer 2.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp3-msg-size *size*

default mtp3-msg-size

default

Resets the the size to the default value which is 4096 (for q.2140) or 272 (for MTP2)

size

size: must be an integer from 1 to 272 for high-speed or low-speed narrowband SS7 links.
size: must be an integer from 1 to 4096 for ATM broadband links.

Usage

Use this command to set the maximum message size, in bytes.

Example

Use this command to set the MTP3 message size to 4096 bytes:

```
mtp3-msg-size 4096
```

mtp3-p1-qlen

Configure the size for the MTP3 p1 queue length.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp3-p1-qlen *size*

default mtp3-p1-qlen

default

Resets the number of size of the priority 1 queue to the default value.

size

size: integer from 1 to 65535. Size should be less than MTP3 p2 qlen and p3 qlen.
Default: 1024

Usage

Use this command to configure the queue length threshold for raising the congestion priority to level 1.

Example

Use this command to set the queue length priority to 128:

mtp3-p1-qlen *128*

mtp3-p2-qlen

Configure the size of the priority 2 queue.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp3-p2-qlen *size*

default mtp3-p2-qlen

default

Resets the number of size of the priority 2 queue to the default value.

size

size: integer from 1 to 65535. Size should be less than MTP3 p3 qlen and greater than p1 qlen.
Default: 1024

Usage

Use this command to configure the queue length threshold for raising the congestion priority to level 2.

Example

Use this command to set the queue length threshold to 256:

mtp3-p2-qlen *256*

mtp3-p3-qlen

Configure the size of the priority 3 queue.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp3-p3-qlen *size*

default mtp3-p3-qlen

default

Resets the number of size of the priority 3 queue to the default value.

size

size: integer from 1 to 65535. Size should be greater than MTP3 p1 qlen and p2 qlen .
Default: 1024

Usage

Use this command to configure the queue length threshold for raising the congestion priority to level 3.

Example

mtp3-p3-qlen *1024*

mtp3-test-pattern

Configures the character string for the test message.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mtp3-test-pattern *pattern*

default mtp3-test-pattern

default

Resets the pattern to the default value.

pattern

pattern: 1 to 15 alphanumeric characters.
Default: SGSN-ORIGINATED

Usage

Use this command to define a test pattern string for the signalling link test match (SLTM).

Example

mtp3-test-pattern *TEST1-HomeOffice*

priority

Configures the MTP3 Link Priority.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

priority *pri_value*

no priority

no

Removes the priority configuration.

pri_value

pri_value: 0 represents highest priority and 15 represents the lowest priority.

Usage

Use this command to configure the link priority within the MTP3 link set.

Example

priority *2*

signaling-link-code

Configures the signaling link code (SLC).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

signaling-link-code *code*

no signaling-link-code

no

Removes the SLC configuration.

code

code: integer from 0 to 15.

Usage

Use this command to uniquely identify the signaling link to be used for MTP3 management messages.

Example

```
signaling-link-code 4
```

sscf-nni-n1

Configures the SSCF NNI N1. This command is only available for ATM-broadband link-types.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sscf-nni-n1 *value*

no sscf-nni-n1

default

Removes the sscf-nni-n1 configuration.

value

value: integer from 1 to 65535.
Default: 1000

Usage

Use this command to identify the network-to-node interface (NNI) between the MTP3 and SSCOP layers.

Example

sscf-nni-n1 *4064*

sscop-max-cc

Configure the maximum value for the SSCOP connection control (CC) state variable. his command is only available for ATM-broadband link-types.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sscop-max-cc *value*

no sscop-max-cc

default

Removes the sscop-max-cc configuration.

value

value: integer from 1 to 65535.
Default: 4

Usage

Use this command as part of the configuration responsible for managing the SSCOP connection. This command sets the number of times retries.

Example

sscop-max-cc *256*

sscop-max-pd

Configures the maximum acceptable value for the SSCOP state variable VT(PD). his command is only available for ATM-broadband link-types.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sscop-max-pd *value*

no sscop-max-pd

default

Removes the **sscop-max-pd** configuration.

value

value: integer from 1 to 65535.
Default: 500

Usage

Use this command to define the maximum number of data PDUs transmitted between POLL PDUs.

Example

sscop-max-pd *2500*

sscop-max-stat

Configures the maximum number of elements included in a status PDU. his command is only available for ATM-broadband link-types.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sscop-max-stat *value*

no sscop-max-stat

default

Removes the **sscop-max-stat** configuration.

value

value: integer from 3 to 65535. This parameter should be an odd integer greater than or equal to 3. Defaultz; 67

Usage

Received in response to a POLL PDU, the STAT PDU includes information about the number of SD PDUs that have been received.

Example

sscop-max-stat *56000*

timeout

This command enables configuration of an array of signaling and flow control timers - for MTP, SSCF, and SSCOP.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] timeout timer timer_value
```

no

Adding **no** to the **timeout** command removes the timer configuration.

timer timer_value

Select the timer and enter a value from the range.
For timers having different ranges for highspeed and lowspeed links or for different variants, the appropriate ranges will be displayed based on the link-type configured.

Important: Currently, the China variant uses ITU values.

Timer	Link Type & Variant	Range of Times Granularity = 100ms	Default Time
mtp2-tmr-t1 Alignment ready timer	Highspeed; ITU	160..3500 (16 - 350 seconds)	3000 (300 seconds)
	Lowspeed; ITU	120 - 500 (12 - 50 seconds)	400 (40 seconds)
	Highspeed; ANSI	160 - 3500 (16 to 350 seconds)	1700 (170 seconds)
	Lowspeed; ANSI	120 - 500 (12 - 50 seconds)	130 (13 seconds)
mtp2-tmr-t2 Not aligned timer	Highspeed; ITU	50 - 1500 (5 - 150 seconds)	50 (5 seconds)
	Lowspeed; ITU	50 - 150 (5 - 15 seconds)	50 (5 seconds)
	Highspeed; ANSI	50 - 1500 (5 - 150 seconds)	230 (23 seconds)
	Lowspeed; ANSI	50 - 150 (5 - 15 seconds)	115 (11.5 seconds)
mtp2-tmr-t3 Aligned timer	Highspeed/Lowspeed; ITU	10 - 140 (1 - 14 seconds)	15 (1.5 seconds)

Timer	Link Type & Variant	Range of Times Granularity = 100ms	Default Time
	Highspeed/Lowspeed; ANSI	10 - 140 (1 - 14 seconds)	115 (11.5 seconds)
mtp2-tmr-t4e Emergency proving period timer	Highspeed; ITU	4 - 60 (400 milliseconds - 6 seconds)	5 (500 milliseconds)
	Lowspeed; ITU	4 - 6 (400 - 600 milliseconds)	5 (500 milliseconds)
	Highspeed; ANSI	4 - 60 (400 milliseconds - 6 seconds)	50 (5 seconds)
	Lowspeed; ANSI	4 - 6 (400 - 600 milliseconds)	6 (600 milliseconds)
mtp2-tmr-t4n Normal proving period timer Once set this timer can be reset but it can not be disabled.	Highspeed; ITU	30 - 700 (3 to 70 seconds)	3 (30 seconds)
	Lowspeed; ITU	20 - 95 (2 - 9.5 seconds)	82 (8.2 seconds)
	Highspeed; ANSI	30 - 700 (3 to 70 seconds)	3 (30 seconds)
	Lowspeed; ANSI	20 - 95 (2 - 9.5 seconds)	23 (2.3 seconds)
mtp2-tmr-t5 Sending status indication busy (SIB) timer	Highspeed/Lowspeed ITU/ANSI	1 - 2 (100 - 200 milliseconds)	1 (100 milliseconds)
mtp2-tmr-t6 Remote congestion timer	Highspeed/Lowspeed ITU/ANSI	10 - 60 (1 to 6 seconds)	30 (3 seconds)
mtp2-tmr-t7 Excessive delay of acknowledgement timer	Highspeed/Lowspeed ITU/ANSI	5 - 20 (500 milliseconds - 2 seconds)	10 (1 second)
mtp2-tmr-t8 Interval timer for error interval monitor timer	Highspeed ITU/ANSI	1 - 2 (100 - 200 milliseconds)	1 (100 milliseconds)
mtp3-tmr-t1 Delay to avoid mis-sequencing on changeover timer	Highspeed/Lowspeed ITU/ANSI	5 - 12 (500 - 1200 milliseconds)	5 (500 milliseconds
mtp3-tmr-t12 Waiting for uninhibit acknowledgement timer	Highspeed/Lowspeed ITU/ANSI	8 - 15 (800 - 1500 milliseconds	8 (800 milliseconds
mtp3-tmr-t13 Waiting for force uninhibit timer	Highspeed/Lowspeed ITU/ANSI	8 - 15 (800 - 1500 milliseconds	8 (800 milliseconds
mtp3-tmr-t14 Waiting for inhibition acknowledgement timer	Highspeed/Lowspeed ITU/ANSI	20 - 30 (2000 - 3000 milliseconds	20 (2000 milliseconds

Timer	Link Type & Variant	Range of Times Granularity = 100ms	Default Time
mtp3-tmr-t17 Delay to avoid oscillation of initial alignment failure and link restart	Highspeed/Lowspeed ITU/ANSI	8 - 15 (800 - 1500 milliseconds	8 (800 milliseconds
mtp3-tmr-t2 Waiting for changeover acknowledgement	Highspeed/Lowspeed ITU/ANSI	7 - 20 (700 - 2000 milliseconds	7 (700 milliseconds
mtp3-tmr-t22 Local inhibit test timer	Highspeed/Lowspeed ITU/ANSI	1800 - 3000 (180 - 300 seconds	1800 (180 seconds)
mtp3-tmr-t23 Remote inhibit test timer	Highspeed/Lowspeed ITU/ANSI	1800 - 3000 (180 - 300 seconds	1800 (180 seconds)
mtp3-tmr-t24 Stabilising timer after removal of local processor outage, used in LPO latching to RPO (national option)	Highspeed/Lowspeed ITU/ANSI	5 - 15 (500 - 1500 milliseconds)	5 (500 milliseconds)
mtp3-tmr-t3 Time controlled diversion-delay to avoid mis-sequencing on changeback	Highspeed/Lowspeed ITU/ANSI	5 - 12 (500 - 1200 milliseconds)	5 (500 milliseconds)
mtp3-tmr-t31 BSN requested timer	Highspeed/Lowspeed ITU/ANSI	50 - 100 (5 to 10 seconds)	50 (5 seconds)
mtp3-tmr-t32 SLT timer	Highspeed/Lowspeed ITU/ANSI	40 - 120 (4 - 12 seconds)	100 (10 seconds)
mtp3-tmr-t33 Connecting timer	Highspeed/Lowspeed ITU/ANSI	50 - 100 (5 to 10 seconds)	50 (5 seconds)
mtp3-tmr-t34 Periodic signalling link test timer	Highspeed/Lowspeed ITU/ANSI	300 - 900 (30 to 90 seconds)	600 (60 seconds)
mtp3-tmr-t4 Waiting for changeback acknowledgement (first attempt)	Highspeed/Lowspeed ITU/ANSI	5 - 12 (500 to 1200 milliseconds)	5 (500 milliseconds)
mtp3-tmr-t5 Waiting for changeback acknowledgement (second attempt)	Highspeed/Lowspeed ITU/ANSI	5 - 12 (500 to 1200 milliseconds)	5 (500 milliseconds)
mtp3-tmr-t7 Waiting for signalling data link connection acknowledgement	Highspeed/Lowspeed ITU/ANSI	10 - 20 (1000 - 2000 milliseconds)	10 (1000 milliseconds)

Timer	Link type & Variant	Range of Times	Default Time
sscf-nni-tmr-t1	ATM Broadband ITU/ANSI	1 - 65535 (10 - 655350 milliseconds) Granularity = 10 ms	500 (5 seconds)
sscf-nni-tmr-t2	ATM Broadband ITU/ANSI	1 - 65535 (10 - 655350 milliseconds) Granularity = 10 ms	3000 (30 seconds)

Timer	Link type & Variant	Range of Times	Default Time
sscf-nni-tmr-t3	ATM Broadband ITU/ANSI	1 - 65535 (10 - 655350 milliseconds) Granularity = 10 ms	1 (10 milliseconds)
sscop-tmr-cc SSCOP CC timer	ATM Broadband ITU/ANSI	1 - 65535 (100 - 6553500 milliseconds) Granularity = 100 ms	2 (200 milliseconds)
sscop-tmr-idle SSCOP idle timer (UNI 3.1 only)	ATM Broadband ITU/ANSI	1 - 65535 (100 - 6553500 milliseconds) Granularity = 100 ms	1 (100 milliseconds)
sscop-tmr-keep-alive SSCOP keep alive timer For stability purposes, tmrKeepAlive >/= tmrPoll and tmrKeepAlive < tmrNoResponse.	ATM Broadband ITU/ANSI	1 - 65535 (100 - 6553500 milliseconds) Granularity = 100 ms	1 (100 milliseconds)
sscop-tmr-no-rsp SSCOP no response timer For stability purposes, tmrNoResponse > tmrKeepAlive.	ATM Broadband ITU/ANSI	1 - 65535 (100 - 6553500 milliseconds) Granularity = 100 ms	15 (1.5 seconds)
sscop-tmr-poll SSCOP poll timer For stability purposes, tmrPoll <= tmrKeepAlive.	ATM Broadband ITU/ANSI	1 - 65535 (100 - 6553500 milliseconds) Granularity = 100 ms	1 (100 milliseconds)

Usage

For a single link and specified link-type (highspeed or lowspeed), this command sets the timer values listed above. The SS7 variant is determined when the SS7 routing domain is first defined from the Global Configuration mode.

Repeat the **timeout** command (one timer and value per entry) as needed to configure all required timers.

Important: Currently, the China variant uses the same timers, values, and defaults as the ITU variant.

Example

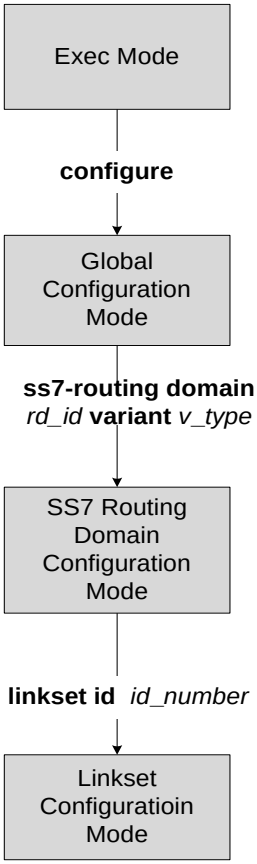
timeout *timer timer_value*

Chapter 168
Linkset Configuration Mode Commands

The Linkset configuration mode defines the MTP3 linkset parameters for a specific SS7 routing domain instance.

In this mode, the prompt will appear similar to:

```
[local]hostname(config-ss7-rd-linkset-<#>)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

adjacent-point-code

This command defines the point-code for the adjacent (next) network element in the SS7 network.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

adjacent-point-code *point-code*

no adjacent-point-code

point-code

Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC range.
- a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

no

Removes the adjacent-point-code configuration for this linkset in the SS7 routing domain

Important: Removing the linkset configuration will result in the termination of all of the links within the linkset.

Usage

Use this command to define the point-code for the adjacent element in the SS7 network.

Example

adjacent-point-code *6.202.7*

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

link

This command creates an MTP3 link configuration for the SS7 linkset and enters the Link configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

link id *id* **[link-type [atm-broadband | highspeed-narrowband | lowspeed-narrowband]**

no link id *id*

no

Disables the specified link configuration.

Important: Removing the link configuration will result in the termination of traffic on the specified link.

#_octets

Sets the number of octets for the length of the LSSU.

id

This number uniquely identifies the link in the linkset.
id: an integer between 1 and 16.

link-type

Identifies the signalling type for this link; options include:

- ATM broadband -- ATM AAL5 over an optical line card (OLC2)
- high speed-narrowband -- 64 kbps over a channelized optical line card (CLC2)
- low speed-narrowband -- 4.8 kbps over a channelized optical line card (CLC2)

Important: Be default link-type is ATM-broadband. To support narrowband SS7, one of the other options must be set.

Usage

Access the Link configuration mode to configure the parameters for the the link.

Example

Access configuration for link 4:

```
link id 4
```

self-point-code

This command defines the SS7 network point-code to identify this SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

self-point-code *point-code*

no self-point-code

point-code

Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC range.
- a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

no

Removes the self-point-code configuration for this linkset in the SS7 routing domain.

Important: Removing the self-point-code will result in the termination of all traffic on this link.

Usage

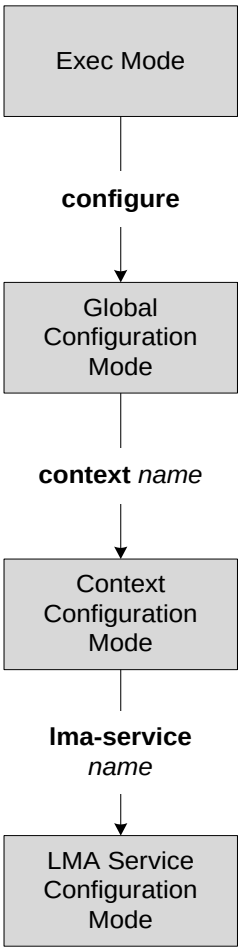
Use this command to define the SS7 point-code to identify this system.

Example

self-point-code *6.192.7*

Chapter 169
LMA Service Configuration Mode Commands

The LMA Service Configuration Mode is used to create and manage the Local Mobility Anchor configuration supporting Proxy Mobile IP on a PDN Gateway in an eHRPD and E-UTRAN/EPC network.



aaa accounting

Enables the LMA to send AAA accounting information for subscriber sessions.

Product

P-GW

Privilege

Administrator

Syntax

```
[ default | no ] aaa accounting
```

default

Sets the command to the default condition of enabled.

no

Disables the ability of the LMA to send AAA accounting information.

Usage

Use this command to enable the LMA service to send all accounting data (start, stop, and interim) to the configured AAA servers.

Important: In order for this command to function properly, AAA accounting must be enabled for the context in which the LMA service is configured using the **aaa accounting subscriber radius** command.

Example

The following command disables aaa accounting for the LMA service:

```
no aaa accounting
```

bind address

Binds the LMA service to a logical IP interface serving as the S2a (HSGW) or S5/S8 (S-GW) interface and specifies the maximum number of subscribers that can access this service over the configured interface.

Product

P-GW

Privilege

Administrator

Syntax

bind address *ipv6_address* **[ipv4-address** *ipv4_address* **] [max-subscribers** *num* **]**

no bind address

no

Removes the interface binding from this service.

address *ipv6_address*

Specifies the IPv6 address of the interface configured as the S2a or S5/S8 interface. *ipv6_address* is specified in colon separated notation.

ipv4-address *ipv4_address*

Specifies optional IPv4 HA/P-GW address to support DSMIP6 session using IPv4 transport. *ipv4_address* must be entered as a standard IPv4 address in dotted decimal notation.

max-subscribers *num*

Default: 3000000
Specifies the maximum number of subscribers that can access this service on this interface. *num* must be configured to an integer between 0 and 3,000,000.

Important: The maximum number of subscribers supported is dependant on the license key installed and the number of active PSCs in the system. A fully loaded system with 13 active PSCs can support 3,000,000 total subscribers. Refer to the license key command and the Usage section (below) for additional information.

Usage

Associate the LMA service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an S2a or S5/S8 interface that provides the session connectivity to an HSGW (S2a) or S-GW (S5/S8). Only one interface can be bound to a service. The interface should be configured prior to issuing this command.
This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.
When configuring the **max-subscribers** option, be sure to consider the following:

- The total number of S2a or S5/S8 interfaces you will configure
- The total number of subscriber sessions that all of the configured interfaces may handle during peak busy hours

- An average bandwidth per session multiplied by the total number of sessions
- The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

Example

The following command would bind the logical IP interface with the address of *4551:0db8:85a3:08d3:3319:8a2e:0370:1344* to the LMA service and specifies that a maximum of *300,000* simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 4551:0db8:85a3:08d3:3319:8a2e:0370:1344 max-subscribers
300000
```

end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Administrator

Syntax `end`

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Administrator

Syntax `exit`

Usage

Return to the previous mode.

mobility-option-type-value

Changes the mobility option type value used in mobility messages.

Product

P-GW

Privilege

Administrator

Syntax

```
mobility-option-type-value { custom1 | standard }

default mobility-option-type-value
```

default

Sets the command to the default value of custom1.

custom1

(Default) Non-standard type values used before they were defined by IANA.

standard

Standard type values as defined by IANA. In addition, standard option uses type values defined in RFC 5844 for HoA options for PMIPv6 PBU/PBA/revocation message.

Usage

Use this command to change the mobility option type value used in mobility messages.

Example

The following command changes the mobility option type value to standard:

```
mobility-option-type-value standard
```

refresh-advice-option

Configures inclusion of a refresh advice option in the binding acknowledgement message sent by the LMA.

Product

P-GW

Privilege

Administrator

Syntax

```
[ default | no ] refresh-advice-option
```

default

Returns the command setting to the default setting of disabled.

no

Disables the inclusion of the refresh advice option in the binding acknowledgement message sent by the LMA

Usage

Use this command to enable the LMA to include this option in a binding acknowledgment sent to the requesting MAG. The option provides a “hint” to the MAG of when it should refresh the binding.
As defined in RFC 3775 “Mobility Support in IPv6”, the binding refresh advice option can only be present in the binding acknowledgement sent from the mobile node's home agent in reply to a registration request. A refresh interval parameter determines the amount of time until the mobile node must send a new registration to the home agent to avoid de-registration and loss of session.

Important: Refer to the refresh-interval-percent and reg-lifetime commands for a complete understanding of registration (binding) lifetimes and refresh intervals.

refresh-interval-percent

Configures percentage of the granted registration lifetime to be used in the refresh interval mobility option in a binding acknowledgement message sent by the LMA service.

Product

P-GW

Privilege

Administrator

Syntax

refresh-interval-percent *number*

default refresh-interval-percent

default

Resets the command value to the default setting of 75.

number

Default: 75
Sets the percent value for session lifetimes for this service.
number must be an integer value from 1 to 99.

Usage

Use this command to configure the amount of the granted registration lifetime to be used in the refresh interval mobility option in the binding acknowledgement message sent by the LMA service to the requesting MAG.
Refreshing a binding or registration is based on the granted registration lifetime. Since a refresh request must be within the granted range of a registration lifetime, this command provides a method of setting the interval of when a refresh request is sent.
As described in RFC 3775 “Mobility Support in IPv6”, if a binding refresh advice option is present in the binding acknowledgement, the refresh interval field in the option must be a value less than the binding lifetime (also returned in the binding acknowledgement). The mobile node then should attempt to refresh its registration at the shorter refresh interval. The home agent will still honor the registration for the lifetime period, even if the mobile node does not refresh its registration within the refresh period.

Important: Refer to the refresh-advice-option and reg-lifetime commands for a complete understanding of registration (binding) lifetimes and refresh intervals.

Example

The following command sets the refresh interval percent to *90*:

```
refresh-interval-percent 90
```

reg-lifetime

Configures the Mobile IPv6 session registration lifetime for this service.

Product

P-GW

Privilege

Administrator

Syntax

reg-lifetime *seconds*

default reg-lifetime

default

Resets the command value to the default setting of 600.

seconds

Default: 600
Sets the time value for session lifetimes for this service.
seconds must be an integer value from1 to 262140.

Usage

Use this command to limit PMIPv6 lifetime on this service. If the PBU contains a lifetime shorter than what is specified, it is granted. If the lifetime is longer, then HA service will limit the granted lifetime to the configured value.

Important: Refer to the refresh-interval-percent and refresh-advice-option commands for a complete understanding of registration (binding) lifetimes and refresh intervals.

Example

The following command sets the registration lifetime for Mobile IPv6 sessions using this service to *1200* seconds (20 minutes):

```
reg-lifetime 1200
```

revocation

Enables the MIP revocation feature and configures revocation parameters.

Product

P-GW

Privilege

Administrator

Syntax

revocation { enable | max-retransmission *number* **| retransmission-timeout** *msecs* **}**

default revocation { enable | max-retransmission | retransmission-timeout }

no revocation enable

default

Resets the keyword to its default value.

no

Disables revocation for this service.

enable

Default: disabled
Enables the MIP registration revocation feature for the LMA service. When enabled, if revocation is negotiated with a MAG and a MIP binding is terminated, the LMA can send a Revocation message to the MAG. This feature is disabled by default.

max-retransmission *number*

Default: 3
The maximum number of retransmissions of a Revocation message before the revocation fails. *number* must be an integer value from 0 through 10.

retransmission-timeout *msecs*

Default: 3000
The number of milliseconds to wait for a Revocation Acknowledgement from the MAG before retransmitting the Revocation message. *msecs* must be an integer value from 500 through 10000.

Usage

Use this command to enable or disable the MIP revocation feature on the LMA or to change settings for this feature.

Example

The following command sets the maximum number of retries for a Revocation message to *6*:

```
revocation max-retransmission 6
```

The following command sets the timeout between retransmissions to *10*:

```
revocation retransmission-timeout 10
```

sequence-number-validate

Configures sequence number validation of the received MIPv6 control packets by the LMA service according to RFC 3775.

Product

P-GW

Privilege

Administrator

Syntax

```
[ default | no ] sequence-number-validate
```

default

Resets the command value to the default setting of enabled.

no

Disables the feature.

Usage

Use this command to configure the sequence number validation of the received MIPv6 control packets (PBUs) by the LMA service. This feature validates MIPv6 control packets and insures that any incoming packets with a sequence number prior to the last number received is consider invalid.
If this service has no cache entry of the home address included in the PBU, it will accept any sequence value in the initial PBU from the mobile node.

setup-timeout

The maximum amount of time allowed for session setup.

Product

P-GW

Privilege

Administrator

Syntax

setup-timeout *seconds*

default setup-timeout

default

Resets the command value to the default setting of 60.

seconds

Default: 60 seconds
The maximum amount of time, in seconds, to allow for setup of a session in this service. *seconds* must be an integer value from 1 through 1000000.

Usage

Use this command to set the maximum amount of time allowed for setting up a session.

Example

The following command sets the maximum time allowed for setting up a session to 5 minutes (300 seconds):

```
setup-timeout 300
```

signalling-packets

Enables the DSCP marking feature for IP headers carrying outgoing signalling packets.

Product

P-GW

Privilege

Administrator

Syntax

signalling-packets ip-header-dscp *value*

[default | no] signalling-packets ip-header-dscp

default

Restores the specified parameter to its default setting of 0x0.

no

Disables the specified functionality.

ip-header-dscp *value*

Used to configure the QoS Differentiated Services Code Point (DSCP) marking for IP header encapsulation. *value*: Represents the DSCP setting. It represents the first six most-significant bits of the ToS field. It can be configured to any hex value from 0x0 through 0x3F. Default is 0x0.

Usage

Use this command to enable or disable the DSCP marking feature for IP headers carrying outgoing signalling packets. DSCP marking is disabled by default.

Example

The following command configures the HSGW service to support DSCP marking for IP headers carrying outgoing signalling packets:

```
signalling-packets ip-header-dscp 0x21
```

simul-bindings

Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address.

Product

P-GW

Privilege

Administrator

Syntax

simul-bindings *number*

default simul-bindings

default

Resets the command value to the default setting of 1.

number

Default: 1
Configures maximum number of "care of" addresses that can be simultaneously bound for the same user as identified by their NAI and home address. *number* must be an integer value between 1 and 3.

Usage

Per RFC 5213 (and 3775), the LMA service creates a binding record known as a binding cache entry (BCE) for each subscriber session it is facilitating. Each BCE is associated with a care-of address. As the mobile node roams, it is possible that the session will be associated with a new care of address.
Typically, the LMA service will delete an old binding and create a new one when the information in the registration request changes. However, the mobile node could request that the LMA maintains previously stored BCEs. This command allows you to configure the maximum number of BCEs that can be stored per subscriber if more than one is requested.

Example

The following command configures the service to support up to 2 addresses per subscriber:

```
simul-bindings 2
```

standalone

Configures the LMA service to start in standalone mode.

Product

P-GW

Privilege

Administrator

Syntax

```
[ default | no ] standalone
```

default

Resets the command value to the default setting.

no

Disables the feature.

Usage

Use this command to start the LMA service in standalone mode.

timestamp-option-validation

Configures validation of timestamp option in binding update messages. By default, timestamp option is mandatory.

Product

P-GW

Privilege

Administrator

Syntax

```
[ default | no ] timestamp-option-validation
```

default

Resets the command value to the default setting of enabled.

no

Disables the feature.

Usage

Use this command to configure timestamp validation in binding update messages.

timestamp-replay-protection

Designates timestamp replay protection scheme as per RFC 4285.

Product

P-GW

Privilege

Administrator

Syntax

timestamp-replay-protection tolerance *seconds*

[default | no] timestamp-replay-protection tolerance

default

Resets the command value to the default setting of 7.

no

Disables the timestamp replay protection feature.

tolerance *seconds*

Default: 7
Defines the acceptable difference in timing (between timestamps) before rejecting packet, in seconds.
seconds must be an integer value between 0 and 65535.

Usage

Use this command to define the acceptable difference in timing (between timestamps) before rejecting packet.

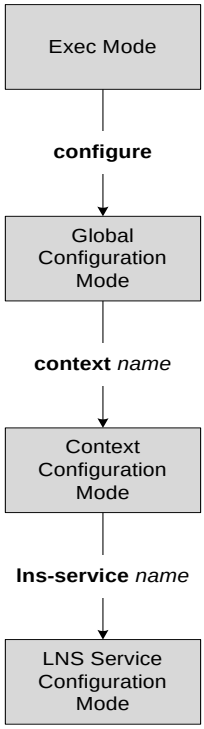
Example

The following command sets the acceptable difference for timestamps to 10 seconds:

```
timestamp-replay-protection tolerance 10
```

Chapter 170
LNS Service Configuration Mode Commands

The LNS Service Configuration Mode is used to create and manage L2TP services within contexts on the system. L2TP Network Server (LNS) services facilitate tunneling with peer L2TP Access Concentrators (LACs).



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

aaa accounting

Enables the sending of authentication, authorization, and accounting (AAA) accounting information by the LNS.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
aaa accounting [ roaming ]

[ no ] aaa accounting
```

no

Disables this option.

accounting [roaming]

Enables the sending of AAA accounting information for subscriber sessions by the LNS, by default is enabled.

roaming: Enables the sending of AAA accounting information by the LNS only for roaming subscribers.

Usage

Use this command to enable the sending of AAA accounting information by the LNS. By default this is enabled.

Example

The following command enables the sending of AAA accounting information by the LNS:

```
aaa accounting
```

authentication

Configures the type of subscriber authentication for PPP sessions terminated at the current LNS.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

authentication { { [allow-noauth] [chap *chap_priority* **] [mschap** *mschap_priority* **] [pap** *pap_priority* **] } | msid-auth }**

allow-noauth

Default: Disabled
Configures the LNS to allow PPP sessions access even though they have not been authenticated. This command issued by itself causes the LNS not to attempt authentication for any PPP sessions.
When the **allow-noauth** option is used in conjunction with commands specifying other authentication protocols and priorities to use, then if attempts to use those protocols fail, the system treats the **allow-noauth** option as the lowest priority.
If no authentication is allowed, the system constructs an Network Access Identifier (NAI) to provide accounting records for the PPP session.

chap *chap_priority*

Default: 1
Configures the LNS to attempt to use Challenge Handshake Authentication Protocol (CHAP) to authenticate the PPP session.
A *chap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.
chap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference.
CHAP is enabled by default as the highest preference.

mschap *mschap_priority*

Default: Disabled
Configures the LNS to attempt to use the Microsoft Challenge Handshake Authentication Protocol (MSCHAP) to authenticate the PPP session.
A *mschap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.
mschap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference.

pap *pap_priority*

Default: 2
This option configures the LNS to attempt to use the Password Authentication Protocol (PAP) to authenticate the PPP session.
A *pap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.
pap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference.
PAP is enabled by default as the second highest preference.

msid-auth

Default: Disabled
This option configures the LNS to attempt to authenticate the PPP session based on the Mobile Station Identity (MSID).

Usage

Use to specify how the LNS service should handle authentication and what protocols to use. The flexibility is given to configure this option to accommodate the fact that not every mobile will implement the same authentication protocols.
By default LNS authentication options are set as follows:

- allow-noauth disabled
- chap enabled with a priority of 1
- mschap disabled
- msid-auth disabled
- pap enabled with a priority of 2

Important: At least one of the keywords must be used to complete the command.

Example

The following command configures the LNS service to allow no authentication for PPP sessions and would perform accounting using the default NAI-construct of username@domain:

```
authentication allow-noauth
```

The following command configures the system to attempt authentication first using CHAP, then MSCHAP, and finally PAP. If the allow-noauth command was also issued, when all attempts to authenticate the subscriber using these protocols failed, then the subscriber would be allowed access:

```
authentication chap 1 mschap 2 pap 3
```

avp map called-number apn

This command maps an incoming Attribute Value Pair (AVP) to a GGSN Access Point Name (APN) for authentication and authorization of the call.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
{ default | no } avp map called-number apn
```

default

Disables mapping.

no

Disables mapping.

Usage

For LNS calls received through a LAC, the ICRQ message includes an APN name in the Called Number AVP. This mapping function enables a GGSN system to provide RADIUS authentication/authorization via a defined APN in place of an LNS configuration. If the mapped APN has not been defined within the GGSN configuration then the call will be rejected.

Example

Enter the following command to enable mapping:

```
avp map called-number apn
```

Enter the following command to disable mapping:

```
no avp map called-number apn
```

bind

This command assigns the IP address of an interface in the current context to the LNS service.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

bind *ip_address* **[max-subscribers** *max_value* **]**

no bind *ip_address*

no

Unassign, or unbind, the local end point to the LNS service.

ip_address

Specifies the IP address of an interface in the current context. This must be a valid IP address entered using IPV4 dotted-decimal notation.

max-subscribers *max_value*

Default: 10000
Specifies the maximum number of subscribers that can be connected to this service at any time. *max_value* must be an integer from 1 through 2500000.

Usage

Use this command to bind the IP address of an interface in the current context to the LNS service.

Example

The following command binds the current context interface IP address *192.168.100.10* to the current LNS service:

```
bind 192.168.100.10
```

The following command removes the binding of the IP address from the LNS service:

```
no bind
```

data sequence-number

Enables data sequence numbering for sessions that use the current LNS service. Data sequence numbering is enabled by default.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[no] data sequence-number
```

no

Disables data sequence numbering for sessions.

Usage

An L2TP data packet header has an optional data sequence numbers field. The data sequence number may be used to ensure ordered delivery of data packets. This command is used to re-enable or disable the use of the data sequence numbers for data packets.

Example

Use the following command to disable the use of data sequence numbering:

```
no data sequence-number
```

Use the following command to re-enable data sequence numbering:

```
data sequence-number
```

default

This command sets the specified LAC service parameter to its default value or setting.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
default { authentication | data sequence-number | ip source-violation | keepalive-
interval | load-balancing | local-receive-window | max-retransmission | max-session-per-
tunnel | max-tunnel-challenge-length | max-tunnels | proxy-lcp-authentication |
retransmission-timeout-first | retransmission-timeout-max | setup-timeout| single-port-
mode | subscriber| trap all tunnel-authentication}
```

authentication

Sets the authentication parameters for PPP sessions to the following defaults:

- allow-noauth disabled
- chap enabled with a priority of 1
- mschap disabled
- msid-auth disabled
- pap enabled with a priority of 2

data sequence-number

Enables data sequence numbering for sessions.

ip source-violation

Sets the IP source violation parameters to the following defaults:

- drop-limit 10
- period 120 seconds
- reneg-limit 5

keepalive-interval

Sets the interval for send L2TP Hello keepalive if there is no control or data transactions to the default value of 60 seconds.

local-receive-window

Sets the window size to be used for the local side for the reliable control transport to the default of 4.

max-retransmission

Sets the maximum number of retransmissions to the default of 5.

max-session-per-tunnel

Sets the maximum number of sessions per tunnel at any point in time to the default of 65535.

max-tunnel-challenge-length

Sets the maximum length of the tunnel challenge to the default of 16 bytes.

max-tunnels

Sets the maximum number of tunnels for this service to the default of 32000.

proxy-lcp-authentication

Sets sending of proxy LCP authentication parameters to the LNS to the default state of enabled.

retransmission-timeout-first

Sets the first retransmit interval to the default of 1 second.

retransmission-timeout-max

Sets the maximum retransmit interval to the default of 8 seconds.

setup-timeout

Sets the maximum time allowed for session setup to the default of 60 seconds.

single-port-mode

Disables assignment of only port 1107 for incoming tunnels and allows dynamic assignment of ports.

subscriber

Sets the name of the default subscriber configuration to use.

tunnel-authentication

Sets tunnel authentication to the default state of enabled.

trap all

Generates all supported SNMP traps.

tunnel-switching

Sets the ability of the LNS to create subsequent tunnels to the default of enabled.

Usage

Use the default command to set LAC service parameters to their default states.

Example

Use the following command to set the keepalive interval to the default value of 60 seconds:

```
default keepalive-interval
```

Use the following command to set the maximum number of sessions per tunnel to the default value of 512:

default max-session-per-tunnel

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

ip source-violation

This command configures settings related to IP source-violation detection.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

ip source-violation { clear-on-valid-packet | drop-limit *num* **| period** *secs* **| reneg-limit** *num* **}**

no ip source-violation clear-on-valid-packet

clear-on-valid-packet

Default: disabled
Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

drop-limit *num*

Default: 10
Sets the number of allowed source violations within a detection period before forcing a call disconnect. If *num* is not specified, the value is set to the default.
num can be an integer from 1 through 1000000.

period *secs*

Default: 120
The length of time (in seconds) for a source violation detection period to last. drop-limit and reneg-limit counters are decremented each time this value is reached.
The counters are decremented in this manner: reneg-limit counter is reduced by one (1) each time the period value is reached until the counter is zero (0); drop-limit counter is halved each time the period value is reached until the counter is zero (0). If *secs* is not specified, the value is set to the default.
secs can be an integer from 1 through 1000000.

reneg-limit *num*

Default: 5
Sets the number of allowed source violations within a detection period before forcing a PPP renegotiation. If *num* is not specified, the value is set to the default.
num can be an integer from 1 through 1000000.

Usage

This function allows the operator to configure a network to prevent problems such as when a user gets handed back and forth between two PDSNs a number of times during a handoff scenario.
When a subscriber packet is received with a source address violation, the system increments both the IP source-violation reneg-limit and drop-limit counters and starts the timer for the IP-source violation period.

Every subsequent packet received with a bad source address during the IP-source violation period causes the reneg-limit and drop-limit counters to increment.
For example, if reneg-limit is set to 5, the system allows five packets with a bad source address (source violations), but on the fifth packet, it re-negotiates PPP.
If the drop-limit is set to 10, the above process of receiving five source violations and renegotiating PPP occurs only once. After the second 5-source violation, the call is dropped. The period timer continues to count throughout this process.
If at any time before the call is dropped, the configured source-violation period is exceeded, the counters for drop-limit is decremented by half and reneg-limit is decremented by 1. See period definition above.

Example

To set the maximum number of source violations before dropping a call to 100, enter the following command:

```
ip source-violation drop-limit 100
```

keepalive-interval

This command specifies the amount of time to wait before sending a Hello keepalive message.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

keepalive-interval *seconds*

no keepalive-interval

no

Disables the generation of Hello keepalive messages on the tunnel.

seconds

Default: 60
Specifies the number of seconds to wait before sending a Hello keepalive message as an integer from 30 through 2147483648.

Usage

Use this command to set the amount of time to wait before sending a Hello keepalive message or disable the generation of Hello keepalive messages completely. A keepalive mechanism is employed by L2TP in order to differentiate tunnel outages from extended periods of no control or data activity on a tunnel. This is accomplished by injecting Hello control messages after a specified period of time has elapsed since the last data or control message was received on a tunnel. As for any other control message, if the Hello message is not reliably delivered then the tunnel is declared down and is reset. The transport reset mechanism along with the injection of Hello messages ensures that a connectivity failure between the LNS and the LAC is detected at both ends of a tunnel.

Example

Use the following command to set the Hello keepalive message interval to *120* seconds:

```
keepalive-interval 120
```

Use the following command to disable the generation of Hello keepalive messages:

```
no keepalive-interval
```

local-receive-window

Specifies the number of control messages the remote peer LAC can send before waiting for an acknowledgement.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

local-receive-window *integer*

integer

Default: 4
Specifies the number of control messages to send before waiting for an acknowledgement as an integer from 1 through 256.

Usage

Use this command to set the size of the control message receive window being offered to the remote peer LAC. The remote peer LAC may send the specified number of control messages before it must wait for an acknowledgment.

Example

The following command sets the local receive window to *10* control messages:

```
local-receive-window 10
```

max-retransmission

Sets the maximum number of retransmissions of a control message to a peer before the tunnel and all sessions within it are cleared.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

max-retransmission *integer*

integer

Default: 5
Specifies the maximum number of retransmissions of a control message to a peer as an integer from 1 through 10.

Usage

Each tunnel maintains a queue of control messages to be transmitted to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval. For example; if the first retransmission occurs after 1 second, the next retransmission occurs after 2 seconds has elapsed, then the next after 4 seconds. If no peer response is detected after the number of retransmissions set by this command, the tunnel and all sessions within are cleared.
Use this command to set the maximum number of retransmissions that the LAC service sends before closing the tunnel and all sessions within. it.

Example

The following command sets the maximum number of retransmissions of a control message to a peer to 7:

```
max-retransmissions 7
```

max-session-per-tunnel

Sets the maximum number of sessions that can be facilitated by a single tunnel at any time.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

max-sessions-per-tunnel *integer*

integer

Default: 512
Specifies the maximum number of sessions as an integer from 1 through 65535.

Usage

Use this command to set the maximum number of sessions you want to allow in a tunnel.

Example

The following command sets the maximum number of sessions in a tunnel to *5000*:

```
max-sessions-per-tunnel 5000
```

max-tunnel-challenge-length

Sets the maximum length of the tunnel challenge in bytes. The challenge is used for authentication purposes during tunnel creation.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

max-tunnel-challenge-length *bytes*

bytes

Default: 16
Specifies the number of bytes to set the maximum length of the tunnel challenge as an integer from 4 through 32.

Usage

Use this command to set the maximum length, in bytes, for the tunnel challenge that is used during tunnel creation.

Example

The following command sets the maximum length of the tunnel challenge to *32* bytes:

```
max-tunnel-challenge-length 32
```

max-tunnels

The maximum number of tunnels that the current LNS service can support.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

max-tunnels *integer*

integer

Default: 32000
Specifies the maximum number of tunnels as an integer from 1 through 32000.

Usage

Use this command to set the maximum number tunnels that this LNS service can support at any one time.

Example

Use the following command to set the maximum number of tunnels for the current LNS service to *20000*:

```
max-tunnels 20000
```

nai-construction domain

Designates the alias domain name to use for Network Access Identifier (NAI) construction.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

nai-construction domain *domain_name* **{ @ | % | - | \ | # | / }**

no nai-construction domain

---

no

Deletes the NAI construction domain alias.

---

domain_name **{ @ | % | - | \ | # | / }**

Specifies the desired domain name alias followed immediately by a separator from the valid list. *domain_name* must be an alphanumeric string of from 1 through 79 characters.

Usage

Use this command to specify the domain alias and separator to use for NAI construction. The specified domain name must be followed by a valid separator (@ | % | - | \ | # | /).

Example

To specify a domain alias of *mydomain@* with a separator of @, enter the following command:

```
nai-construction domain mydomain@
```

To delete the current setting for the NAI construction domain alias, enter the following command:

```
no nai-construction domain
```

newcall

Configures new call related behavior.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
newcall duplicate-subscriber-requested-address { accept | reject }

default newcall duplicate-subscriber-requested-address
```

duplicate-subscriber-requested-address

Configures how duplicate sessions with same address request are handled

default

Sets or restores default value assigned for specified parameter

Example

The following command configures new call with duplicate address request to accept:

```
newcall duplicate-subscriber-requested-address accept
```

peer-lac

Adds a peer LAC address for the current LNS service. Up to eight peer LACs can be configured for each LNS service.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

peer-lac { *ip_address* | *ip_address*/*mask* } [encrypted] secret *secret* [description *text*]

no peer-lac *ip_address*

no peer-lac *ip_address*

Deletes the peer LAC IP address specified by *ip_address*. *ip_address* must be entered using IPv4 dotted-decimal notation.

ip_address

The IP address of a specific peer LAC for the current LNS service. *ip_address* must be entered using IPv4 dotted-decimal notation.

ip_address/*mask*

A network prefix and mask enabling communication with a group of peer LACs. *ip_address* is the network prefix expressed in IPv4 dotted-decimal notation.
mask is the number of bits that defines the prefix.

[encrypted]

Specifies the encrypted shared key between the LAC and the LNS service.
This keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

secret *secret*

Designates the secret which is shared between the current LNS service and the peer LAC. *secret* must ben alphanumeric string of 1 through 127 characters that is case sensitive.

description *text*

Specifies the descriptive text to use to describe the specified peer LAC. *text* must be an alphanumeric string of 0 through 79 characters.

Usage

Use this command to add a peer LAC address for the current LNS service.

Specific peer LACs can be configured by specifying their individual IP addresses. In addition, to simplify configuration, communication with a group of peer LACs can be enabled by specifying a network prefix and a mask.

Example

The following command adds a peer LAC to the current LNS service with the IP address of *10.10.10.100*, and specifies the shared secret to be *1b34nnf5d*:

```
peer-lac 10.10.10.100 secret 1b34nnf5d
```

The following command enables communication with up to 16 peer LACs on the 192.168.1.0 network each having a secret of *abc123*:

```
peer-lac 92.168.1.0/28 secret abc123
```

The following command removes the peer LAC with the IP address of *10.10.10.200* for the current LNS service:

```
no peer-lac 10.10.10.200
```

proxy-lcp-authentication

Enables/disables proxy LCP authentication.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[no] proxy-lcp-authentication
```

no

Disables the processing of proxy LCP authentication parameters from the LAC.

proxy-lcp-authentication

Default: Enabled
Enables the processing proxy LCP authentication parameters from the LAC.

Usage

When enabled, if proxy LCP authentication parameters are received from the LAC and are acceptable, the LNS resumes the PPP session from the authentication phase and goes to the IPCP phase.
When disabled, PPP is always started from the LCP phase, ignoring and discarding any proxy LCP authentication parameters received from the LAC. Disable this feature in situations where accept proxy LCP Auth AVPs that the peer LAC sends should not be expected.

Example

Use the following command to disable the processing of proxy LCP authentication parameters from the LAC:

```
no proxy-lcp-authentication
```

Use the following command to re-enable the processing of proxy LCP authentication parameters from the LAC:

```
proxy-lcp-authentication
```

retransmission-timeout-first

Configures the initial timeout for the retransmission of control messages to the peer LAC.

Privilege

Security Administrator, Administrator

Syntax

retransmission-timeout-first *integer*

integer

Default: 1
Specifies the amount of time (in seconds) to wait before sending the first control message retransmission. This value is an integer from 1 through 100.

Usage

Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted.

Example

The following command sets the initial retransmission timeout to 3 seconds:

```
retransmission-timeout-first 3
```

retransmission-timeout-max

Configures the maximum amount of time that can elapse before retransmitting control messages to the peer LAC.

Privilege

Security Administrator, Administrator

Syntax

retransmission-timeout-max *integer*

integer

Default: 8
Specifies the maximum time (in seconds) to wait before retransmitting control messages. If this limit is reached, the tunnel, and all sessions within it, is cleared. This value is an integer from 1 through 100.

Usage

Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval. For example; if the first retransmission occurs after 1 second, the next retransmission occurs after 2 seconds has elapsed, then the next after 4 seconds. This continues until the limit set by this command is reached. If this limit is reached, the tunnel, and all sessions within it, is cleared.

Example

Use the following command to set the maximum retransmission time-out to *10* seconds:

```
retransmission-timeout-max 10
```

setup-timeout

Configures the maximum amount of time, in seconds, allowed for session setup.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

setup-timeout *seconds*

seconds

Default: 60
Specifies the maximum time (in seconds) to wait for the setup of a session. *seconds* must be an integer from 1 through 1000000.

Usage

This command controls the amount of time allowed for tunnel establishment with a peer LAC. If this timer is exceeded the tunnel setup is aborted.

Example

The following command configures a maximum setup time of *120* seconds:

```
setup-timeout 120
```

single-port-mode

When enabled, this command sets the LNS to use only the default local UDP port (port 1701) for the life of a tunnel.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[no | default] single-port-mode
```

no

Disable single port mode

Usage

Use this command to control the L2TP LNS tunnel local UDP port assignment mode. If single-port-mode is enabled, the LNS-service uses the standard UDP port (port 1701) for the life of the incoming tunnel. Otherwise, it assigns a new local UDP port number for a tunnel when it responds to a tunnel create request received on the standard port number. This is done for load distributing the tunnel processing between multiple tasks within the system to increase the capacity and performance. Even though all L2TP LACs are required to support such dynamic port assignments during tunnel establishments, there exist some LACs that do not support port assignment other than port 1701. This single-port-mode feature can be enabled to support such LAC peers. This configuration must be applied for the LNS-Service before the **bind** command is executed.

Example

The following command enables single port mode for the current LNS service:

```
single-port-mode
```

trap

This command generates SNMP traps.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[no] trap all
```

no

Disables SNMP traps.

Usage

Use this command to enable/disable all supported SNMP traps.

Example

To enable all supported SNMP traps, enter the following command;

```
trap all
```

tunnel-authentication

Enables/disables L2TP tunnel authentication for the LNS service.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[no] tunnel-authentication
```

no

Disables tunnel authentication
Tunnel authentication is enabled by default.

Usage

When tunnel authentication is enabled, a configured shared secret is used to ensure that the LNS service is communicating with an authorized peer LAC. The shared secret is configured by the **peer-lac** command, the **tunnel l2tp** command in the Subscriber Configuration mode, or the **Tunnel-Password** attribute in the subscribers RADIUS profile.

Example

To disable tunnel authentication, use the following command:

```
no tunnel-authentication
```

To re-enable tunnel authentication, use the following command:

```
tunnel-authentication
```

tunnel-switching

Enables or disables the LNS service from creating tunnels to another LAC for an existing tunnel.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[no] tunnel-switching
```

no

Disable tunnel switching.
Tunnel switching is enabled by default.

Usage

Tunnel switching is when the LNS has a tunnel connected to a LAC and creates a tunnel to a different LAC and routes the data from the original LAC through the new tunnel to the other LAC.

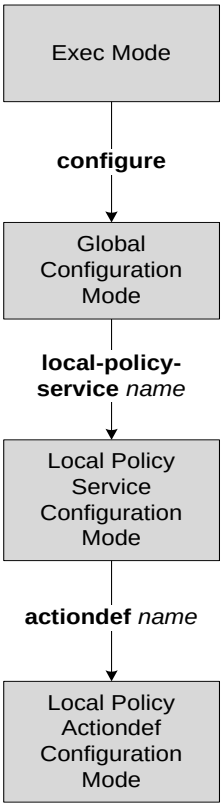
Example

To disable tunnel switching in the LNS, enter the following command;

```
no tunnel-switching
```

Chapter 171
Local Policy Actiondef Configuration Mode Commands

The Local Policy Actiondef Configuration Mode is used to define the action definitions to be used for local QoS policies.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

action

This command configures the action priority for an actiondef.

Product

P-GW

Privilege

Security Administrator, Administrator

Syntax

action priority *priority action_name arguments*

no action priority *priority*

---

priority *priority*

Specifies a priority for the specified action.
priority must be a unique integer from 1 to 2048.

---

action_name arguments

The following actions are supported. *arguments* specifies a set of parameters to be used when invoking the action.

- **activate-ambr uplink** *bandwidth* **downlink** *bandwidth*

  Sets the aggregated maximum bit rate (AMBR) for the APN.

  Configures uplink and downlink bandwidth. *bandwidth* must be an integer from 1 to 1000000000.

- **activate-flow-detection { initiation | termination } ruledef** *ruledef_name*

  Detects a flow and takes action.

  initiation ruledef: Checks for flow initiation and adds a rule definition.

  termination ruledef: Checks for flow termination and adds a rule definition.

  ruledef_name must be an existing ruledef.

- **activate-policy-group**

  Not supported in this release.

- **activate-rule name** *rule_name*

  Activates a rule within ECS rulebase for a subscriber.

  rule_name must be an existing rule within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

- **activate-rulebase name** *rulebase_name*

  Associates the session with a specific rulebase.

  rulebase_name must be an existing rulebase within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

- **allow-requested-qos**

  Allow a specific UE initiated QoS request.

- **allow-session**

Allows the session to continue.

- **create-bearer qci** *value* **arp** *value* **uplink-mbr** *mbr_rate* **downlink-mbr** *mbr_rate* **[uplink-gbr** *gbr_rate* **] downlink-gbr** *gbr_rate*

  Creates a bearer with a specific QCI and BANDWIDTH.

  qci *value* must be an integer from 1 through 254.

  arp *value* must be an integer from 1 through 15 (StarOS v12.1 and earlier) or 1 through 127 (StarOS v12.2 and later).

  uplink-mbr: Uplink maximum bitrate. *mbr_rate* must be an integer from 1 through 1000000000.

  downlink-mbr: Downlink maximum bitrate. *mbr_rate* must be an integer from 1 through 1000000000.

  uplink-gbr: Uplink guaranteed bitrate. *gbr_rate* must be an integer from 1 through 1000000000.

  downlink-gbr: Downlink guaranteed bitrate. *gbr_rate* must be an integer from 1 through 1000000000.

- **deactivate-ambr**

  Removes AMBR control for the specific session.

- **deactivate-flow-detection { initiation | termination } ruledef** *ruledef_name*

  Deactivates detection of flow and takes action.

  initiation ruledef: Checks for flow initiation and adds a rule definition.

  termination ruledef: Checks for flow termination and adds a rule definition.

  ruledef_name must be an existing ruledef.

- **deactivate-policy-group**

  Not supported in this release.

- **deactivate-rule name** *rule_name*

  Deactivates a rule within ECS.

  rule_name must be an existing rule within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

- **deactivate-rulebase name** *rulebase_name*

  Disassociates the rulebase from a session.

  rulebase_name must be an existing rulebase within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

- **default-qos qci** *value* **arp** *value*

  Sets the default QoS parameters for the session

  qci *value* must be an integer from 1 through 254.

  arp *value* must be an integer from 1 through 15 (StarOS v12.1 and earlier) or 1 through 127 (StarOS v12.2 and later).

- **delete-bearer qci** *value* **arp** *value*

  Deletes a bearer

  qci *value* must be an integer from 1 through 254.

arp *value* must be an integer from 1 through 15 (StarOS v12.1 and earlier) or 1 through 127 (StarOS v12.2 and later).

- **reject-requested-qos**

  Reject UE QoS resource request.

- **terminate-session**

  Terminates the session.

no action priority *priority*

Deletes the specified action.

Usage

Use this command to enable the setting of parameters to be used when invoking actions. Actions are a series of operations that are triggered by activated rules.
This command can be entered multiple times to configure multiple actions for an actiondef. The actions are examined in priority order until a match is found and the corresponding action is applied.

Example

The following command creates an action to allow a session to continue with priority set to *125*:

```
action priority 125 allow-session
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

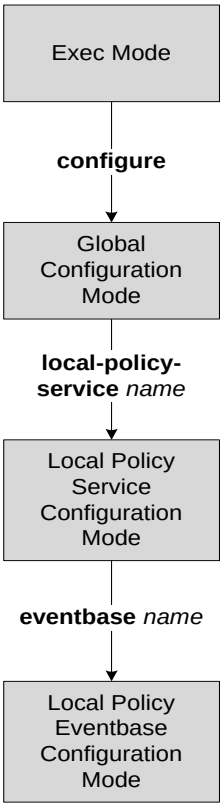
```
exit
```

Usage

Use this command to return to the parent configuration mode.

Chapter 172
Local Policy Eventbase Configuration Mode Commands

The Local Policy Eventbase Configuration Mode is used to configure the events to be used for local QoS policies.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

rule

This command enables the setting of event rules. An event is something that occurs in the system which would trigger a set of actions to take place, such as new-call or rat-change.

Product

P-GW

Privilege

Security Administrator, Administrator

Syntax

rule priority *priority* **[event** *list_of_events* **] ruledef** *ruledef_name* **actiondef** *actiondef_name* **[continue]**

no rule priority *priority*

---

priority *priority*

Specifies a priority for the specified rule.
priority must be unique and an integer from 1 to 2048.

---

event *list_of_events*

The event is defined by any of the following events. Upon triggering the event, the rules specified in the eventbase are executed.

- **default-qos-change**: The event is triggered as a result of a default QoS change.
- **location-change**: The event is triggered as a result of any change relating to location.
- **new-call**: This event is initiated when a new call is established.
- **out-of-credit**: This event is initiated on out of OCS credit.
- **realloc-of-credit**: This event is initiated on OCS reallocation of credit
- **request-qos**: This event is initiated as the result of UE requested QoS.
- **service-flow**: The event is triggered as a result of a new service flow being detected for the subscriber.

---

ruledef *ruledef_name*

Associates the rule with a specific ruledef.
ruledef_name must be an existing ruledef within this local QoS policy service.

---

actiondef *actiondef_name*

Associates the rule with a specific actiondef.
actiondef_name must be an existing actiondef within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

---

continue

Subsequent rules are also matched; otherwise, rule evaluation is terminated on first match.

no rule priority *priority*

Deletes the specified rule.

Usage

Use this command to create, configure, or delete event rules.
The rules are executed in priority order, and if the rule is matched the action specified in the actiondef is executed. If an event qualifier is associated with a rule, the rule is matched only for that specific event. If a qualifier of **continue** is present at the end of the rule, the subsequent rules are also matched; otherwise, rule evaluation is terminated on first match.
This command can be entered multiple times to configure multiple rules for an eventbase.

Important: A maximum 256 rules are suggested in an eventbase for performance reasons.

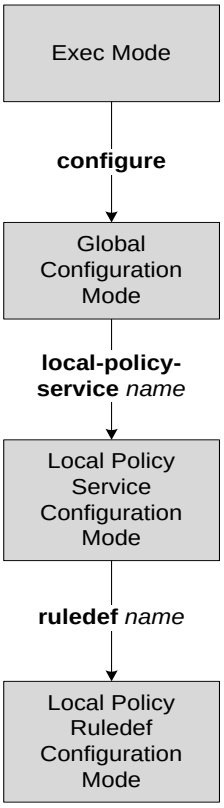
Example

The following command creates a rule with priority set to *2* and associated with **ruledef** *rule5* and **actiondef** *action7*:

```
rule priority 2 ruledef rule5 actiondef action7
```

Chapter 173
Local Policy Ruledef Configuration Mode Commands

The Local Policy Ruledef Configuration Mode is used to configure the rule definitions to be used for local QoS policies.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

condition

This command is used to configure the conditions which trigger the ruledef event.

Product

P-GW

Privilege

Security Administrator, Administrator

Syntax

```
condition priority priority { variable { eq | ge | gt | le | lt | match | ne | nomatch }
regex | string_value | int_value | set }

no condition priority priority
```

priority *priority*

Specifies a priority for the specified condition.
priority must be unique and an integer from 1 to 2048.

variable

The following variables are supported:

- **apn**

  The APN associated with the current session expressed as an alphanumeric string of 1 through 63 characters.

- **arp**

  The APN associated with the current session expressed as an integer from 1 through 15.

- **bandwidth**

  Total bandwidth associated with the QCI and ARP value associated with the request, expresed as an integer from 0 through 1000000000.

- **date**

  Date value to match. <Clock in format YYYY:MM:DD>

- **day-of-month**

  The day of the month to match the rule to, expressed as an integer from 1 through 31.

- **day-of-week**

  Sunday...Saturday, expressed as an integer from 1 to 7.

- **imeisv**

  IMEISV of the user equipment expressed as an alphanumeric string of 1 through 63 characters.

- **imsi**

  IMSI associated with the subscriber expressed as an alphanumeric string of 1 through 63 characters.

- **meid**

  MEID associated with the subscriber expressed as an alphanumeric string of 1 through 63 characters.

- **month-of-year**

Jan, Feb….Dec, expressed as an integer from 1 through 12.

- **msisdn**

  MSISDN associated with the session expressed as an alphanumeric string of 1 through 63 characters.

- **nai**

  NAI associated with the session expressed as an alphanumeric string of 1 through 63 characters.

- **pdn-count**

  Number of PDNs associated with the same APN, expressed as an integer from 0 through 1000000000.

- **qci**

  QCI associated with the current event expressed as an nteger from 1 through 254.

- **radio-access-technology**

  Radio access technology associated with the subscriber:

  - **cdma-1xrtt**: CDMA 1X RTT radio access technology
  - **cdma-evdo**: CDMA-EVDO radio access technology
  - **cdma-evdo-reva**: CDMA EVDO REVA radio access technology
  - **cdma-other**: Other CDMA radio access technologies
  - **ehrpd**: EHRPD radio access technology
  - **eutran**: EUTRAN radio access technology
  - **gan**: GAN radio access technology
  - **gprs-geran**: GPRS GERAN radio access technology
  - **gprs-other**: Other GPRS radio access technology
  - **hspa**: HSPA radio access technology
  - **unknown**: Unknown radio access technology
  - **wcdma-utran**: WCDMA UTRAN radio access technology
  - **wimax**: WiMax radio access technology
  - **wireless-lan**: Wireless LAN radio access technology

- **serving-node-address**

  IP address associated with the current node serving the subscriber entered using IPv4 dotted-decimal or IPv6 colon-separated notation.

- **serving-plmn**

  PLMN associated with the current node serving the subscribe expressed as an alphanumeric string of 1 through 63 characters.

- **time-of-day**

  Time associated with the change. <Clock in format HH:mm:ss or HH:mm >

---

eq | ge | gt | le | lt | match | ne | nomatch

eq: Operation equal to
ge: Operation greater than or equal to
gt: Operation greater than

le: Operation less than or equal to
lt: Operation less than
match: Operation match
ne: Operation not equal to
nomatch: Operation nomatch

no condition priority *priority*

Deletes the specified condition.

Usage

Use this command to configure the conditions which trigger the ruledef event. A ruledef represents a set of matching conditions.
This command can be entered multiple times to configure multiple conditions for a ruledef. The conditions are examined in priority order until a match is found and the corresponding condition is applied.

Example

The following command creates a condition with priority set to *5* and configured match apn *myapn**:

```
condition priority 5 apn match myapn*
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

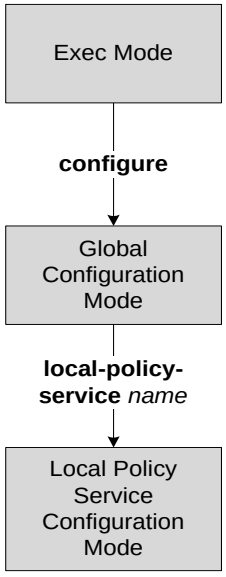
Usage

Use this command to return to the parent configuration mode.

Chapter 174
Local Policy Service Configuration Mode Commands

The Local Policy Service Configuration Mode is used to configure the local QoS policy for one or more services.

Important: A maximum of 16 local QoS policy services are supported.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

actiondef

This command enables creating, configuring, or deleting action definitions for an event.

Product

P-GW

Privilege

Security Administrator, Administrator

Syntax

actiondef *actiondef_name* **[-noconfirm]**

no actiondef *actiondef_name*

no

Deletes the specified actiondef from the local QoS policy service.

actiondef_name

Specifies name of the actiondef.
actiondef_name must be unique within the service expressed as an alphanumeric string of 1 through 63 characters.
If the named actiondef does not exist, it is created, and the CLI mode changes to the Local Policy Actiondef Configuration Mode wherein the actiondef can be configured.
If the named actiondef already exists, the CLI mode changes to the Local Policy Actiondef Configuration Mode for that actiondef.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create, configure, or delete an actiondef. The actiondef configuration is used to configure the action definitions for an event. The event ruledef will have one or more rules and associated action(s).
This command can be entered multiple times to specify multiple actiondefs.

Important: A maximum of 256 actiondefs are suggested in a local QoS policy service for performance reasons. An actiondef can be referenced by multiple eventbases.

Entering this command results in the following prompt:

```
[context_name]hostname(config-local-policy-actiondef)#
```

Local Policy Actiondef Configuration Mode commands are defined in the *Local Policy Actiondef Configuration Mode Commands* chapter.

Example

The following command creates an actiondef named *actiondef1* and enters the Local Policy Actiondef Configuration Mode:

```
actiondef actiondef1
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

eventbase

This command enables creating, configuring, or deleting an eventbase.

Product

P-GW

Privilege

Security Administrator, Administrator

Syntax

eventbase *eventbase_name* **[-noconfirm]**

no eventbase *eventbase_name*

no

Deletes the specified eventbase from the local QoS policy service.

eventbase_name

Specifies name of the eventbase.
eventbase_name must be unique within the service expressed as an alphanumeric string of 1 through 63 characters.

Important: Currently, only one eventbase is supported, and it must be named "default".

If the named eventbase does not exist, it is created, and the CLI mode changes to the Local Policy Eventbase Configuration Mode wherein the eventbase can be configured.
If the named eventbase already exists, the CLI mode changes to the Local Policy Eventbase Configuration Mode for that eventbase.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create, configure, or delete an eventbase.
Entering this command results in the following prompt:

```
[context_name]hostname(config-local-policy-eventbase)#
```

Local Policy Eventbase Configuration Mode commands are defined in the *Local Policy Eventbase Configuration Mode Commands* chapter.

Example

The following command creates an eventbase named *default* and enters the Local Policy Eventbase Configuration Mode:

```
eventbase default
```

ruledef

This command enables creating, configuring, or deleting a rule definition.

Product

P-GW

Privilege

Security Administrator, Administrator

Syntax

ruledef *ruledef_name* **[-noconfirm]**

no ruledef *ruledef_name*

no

Deletes the specified ruledef from the local QoS policy service.

ruledef_name

Specifies name of the ruledef.
ruledef_name must be unique within the service expressed as an alphanumeric string of 1 through 63 characters.
If the named ruledef does not exist, it is created, and the CLI mode changes to the Local Policy Ruledef Configuration Mode wherein the ruledef can be configured.
If the named ruledef already exists, the CLI mode changes to the Local Policy Ruledef Configuration Mode for that ruledef.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create, configure, or delete a ruledef. A ruledef represents a set of matching conditions. This command can be entered multiple times to specify multiple ruledefs.

Important: A maximum 256 ruledefs are suggested in a local QoS policy service for performance reasons.

Entering this command results in the following prompt:

```
[context_name]hostname(config-local-policy-ruledef)#
```

Local Policy Ruledef Configuration Mode commands are defined in the *Local Policy Ruledef Configuration Mode Commands* chapter.

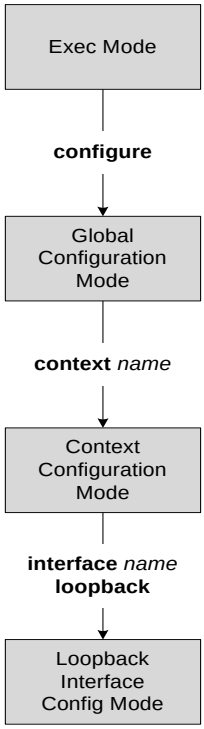
Example

The following command creates a ruledef named *rule5* and enters the Local Policy Ruledef Configuration Mode:

```
ruledef rule5
```

Chapter 175
Loopback Interface Configuration Mode Commands

Use the Loopback Interface Configuration mode to create and manage loopback interfaces that provide IP addresses that are always available and reachable from any interface within a given context.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

crypto-map

Applies the specified IPSec crypto-map to this interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

crypto-map *map_name* **[secondary-address** *sec_ip_addr* **]**

no

Deletes the application of the crypto map on this interface.

map_name

Specifies the name of the crypto map being applied. The name is an alphanumeric string of 1 through 127 characters that is case sensitive.

secondary-address *sec_ip_addr*

Applies the crypto map to the secondary address for this interface that is specified by *sec_ip_addr*. *sec_ip_addr* must be specified using the IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

In order for ISAKMP and/or manual crypto maps to work, they must be applied to a specific interface using this command. Dynamic crypto maps should **not** be applied to interfaces.
The crypto map must be configured in the same context as the interface.

Example

To apply the IPSec crypto map named cmap1 to this interface, use the following command:

```
crypto-map cmap1
```

description

Use this command to configure the descriptive text for the current interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

description *text***no description**

no

Clears the description for the interface.

text

Specifies the descriptive text to use. For *text*, enter an alphanumeric string of 0 through 79 characters. If spaces or special characters are required, the stirng must be bracketed with double quotation marks.

Usage

Set the description to provide any useful information on the interface's primary function, services, end users.

Example

```
description sampleInterfaceDescriptiveText
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

ip address

Use this command to configure the IP options for the current interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip address { *ip_address ip_mask* | *ip_address/bitmask* **} [secondary | srp-activate]**

no ip address ip_address

no

Deletes the IP address you specify from the interface configuration.

address {*ip_address ip_mask* | *ip_address/bitmask***} [secondary | srp-activate]**

Configures the IP address and network mask for the interface.
Enter an *ip_address ip_mask* to specify an IP address and the subnet mask pair that identifies the IP address of the interface. *ip_address* is entered in IPv4 dotted-decimal or IPv6 colon-separated notation. Currently, the only value accepted for *ip_mask* is 255.255.255.255 (IPv4) or 120 (IPv6) .
For the network mask, *ip_address/net_mask*, enter the IP address and the length in bits of the network mask, Fo example, 192.168.1.0/32 (IPv4) or fe80::c0a8:100/32 (IPV6). Currently, the only value accepted for bit_mask is 32.
Use the **secondary** keyword ito configure a secondary IP address on the interface. This is referred to as multi-homing of the interface.
Use the **srp-activate** keyword to activate the IP address for Interchassis Session Recovery (ICSR).

Usage

Create and manage loopback interfaces for the current context.

Example

The following command configures IP address to associate with the interface:

```
ip address 1.2.3.4 255.255.255.255
```

The following command removes the associated IP address for the interface:

```
no ip address 10.2.3.4
```

ip vrf

Use this command to configure the IP VPN Routing Forwarding (VRF) instance for the current interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip vrf forwarding *vrf_name***no vrf forwarding**

no

Deletes the IP VRF instance you specify from the interface configuration.

vrf_name

Specifies the preconfigured IP VRF instance name to be used with this interface.
For *vrf_name*, enter a VRF instance name that was preconfigured via the **ip vrf forwarding** command in Context Configuration mode.

Usage

Use this command to associate a preconfigured IP VRF instance for the current interface.

Example

The following command associates a preconfigured IP VRF instance named *vrf_1* with this interface:

```
ip vrf forwarding vrf_1
```

ipv6 address

Use this command to configure the IPv6 options for the current interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ipv6 address *ipv6_address ip_mask* **[srp-activate]**

no iv6p address *ipv6_address*

no

Deletes the specified IPv6 address from the interface configuration.

address *ipv6_address ip_mask* **[srp-activate]**

Configures the IP address and network mask for the interface.
ipv6_address ip_mask specifies an IP address and the subnet mask pair that identifies the IPv6 address of the interface. Specify *ipv6_address* in IPv6 colon-separated notation.
The **srp-activate** keyword activates the IPv6 address for Session Recovery.

Usage

Create and manage loopback interfaces for the current context and enable Session Redundancy Protocol (SRP) when appropriate.

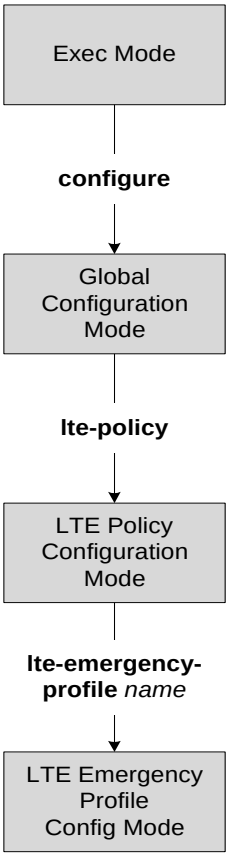
Example

The following command configures an IPv6 address to associate with the interface and enables SRP:

```
ipv6 address 2001:268:2008:b::1021/128 srp-activate
```

Chapter 176
LTE Emergency Profile Configuration Mode Commands

This mode configures parameters supporting the IP Multimedia Subsystem (IMS) emergency bearer services. Connectivity to an emergency Packet Data Network (PDN) is statically configured in this mode.



ambr

Configures the maximum aggregated uplink and downlink bitrate values for this profile.

Product

MME

Privilege

Administrator

Syntax

ambr max-ul *bitrate* **max-dl** *bitrate*

no ambr

no

Removes the aggregated maximum bitrate (AMBR) configuration for this emergency profile.

max-ul *bitrate*

Configures the maximum aggregated bitrate value for the uplink as an integer from 0 through 1410065408.

max-dl *bitrate*

Configures the maximum aggregated bitrate value for the downlink as an integer from 0 through 1410065408.

Usage

Use this command to configure uplink and downlink maximum aggregated bitrate values to be shared across all non-guaranteed bitrate bearers established for the emergency session.

Example

The following example configures the uplink AMBR value to *2000* bps and the downlink AMBR value to *2000* bps:

```
ambr max-ul 2000 max-dl 2000
```

apn

Configures the name and PDN type of the access point name (APN) used for emergency PDN connections.

Product

MME

Privilege

Administrator

Syntax

apn *apn_name* **pdn-type { ipv4 | ipv4v6 | ipv6 }**

no apn

no

Removes the selected APN from the profile.

apn_name

apn_name specifies the name of a pre-configured APN profile to associate with this LTE emergency profile. For more information on APNs, refer to the **apn** command in the *Context Configuration Mode Commands* chapter.

pdn-type { ipv4 | ipv4v6 | ipv6 }

Configures the packet data network type supported by the APN and this profile.
ipv4: Specifies that the PDN supports IPv4 network traffic.
ipv4v6: Specifies that the PDN supports both IPv4 and IPv6 network traffic.
ipv6: Specifies that the PDN supports IPv6 network traffic.

Usage

Use this command to select the APN to be used for emergency bearer services. APNs are configured through the APN Configuration mode. For more information regarding APN configuration mode commands, refer to the *APN Configuration Mode Commands* chapter.

Example

The following command specifies that the APN named *apn-3.com* is to be used for emergency bearer services and that the PDN supports IPv4 traffic only:

```
apn apn-3.com pdn-type ipv4
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

pgw

Statically configures a P-GW to support emergency bearer services for this profile.

Product

MME

Privilege

Administrator

Syntax

pgw fqdn *fqdn*

pgw ip-address *address* **protocol { both | gtp | pmip } weight** *value*

no pgw { fqdn | ip-address *address* **}**

no *fqdn*

Removes the specified P-GW Fully Qualified Domain Name (FQDN) or IP address from this profile.

fqdn *fqdn*

Specifies the domain name of the P-GW as an alphanumeric string of 1 through 256 characters.

Important: A maximum of one P-GW FQDN configuration is allowed per profile.

ip-address *address*

Specifies the IP address for the P-GW in IPv4 dotted-decimal or IPv6 colon-separated notation.

Important: A maximum of four P-GW IP address configurations are allowed per profile.

protocol { both | gtp | pmip }

Specifies the protocol the P-GW supports. Options are:

- **both**: Specifies that both the GTP and PMIP protocols are supported.
- **gtp**: Specifies that only GTP is supported.
- **pmip**: Specifies that only PMIP is supported.

weight *value*

Assigns a weight to P-GW IP address to use as a preferred P-GW as an integer from 1 through 100. Lowest value has the least preference.

Usage

Use this command to statically configure the P-GW used to support emergency bearer services through this profile.

Example

The following command configures the P-GW supporting emergency bearer services for this profile as *pdn-911.gov*:

```
pgw fqdn P-GW FQDN
```

The following command configures the P-GW supporting emergency bearer services for this profile as having an IPv4 address of *10.2.3.4*, supporting GTP only, and having a weight of *10*:

```
pgw ip-address 10.2.3.4 protocol gtp weight 10
```

qos

Configures the quality of service (QoS) parameters for the emergency bearer service.

Product

MME

Privilege

Administrator

Syntax

qos qci *qci* **arp** *arp_value* **preemption-capability { may | shall-not } vulnerability { not-preemptable | preemtable }**

no qos

qci *qci*

Specifies the QoS Class Identifier (QCI) for the emergency bearer profile as an integer from 0 through 255.

arp *arp_value*

Defines the address retention priority value as an integer from 1 through 15.

preemption-capability { may | shall-not }

Specifies the preemption capability flag. Options are:

- **may**: Bearer may be preempted
- **shall-not**: Bearer shall not be preempted

vulnerability { not-preemptable | preemptable }

Specifies the vulnerability flag. Options are:

- **not-preemptable**: Bearer cannot be preempted.
- **preemptable**: Bearer can be preempted.

Usage

Use this command to set the QoS ARP and QCI parameters for the emergency bearer configuration.

Example

The following command sets the QCI number to *7*, the ARP value to *2* the preemption capability to “may”, and the vulnerability flag to “pre-emptable”:

```
qos qci 7 arp 2 preemption-capability may vulnerability preemptable
```

ue-validation-level

Configures the type of user equipment (UE) that can use the emergency bearer service through the profile.

Product

MME

Privilege

Administrator

Syntax

```
ue-validation-level { auth-only | full | imsi | none }

default ue-validation-level
```

default

Returns the command to its default setting of "none".

{ auth-only | full | imsi | none }

Specifies the type of UE allowed to use the emergency bearer service. Options are:

- **auth-only**: Specifies that UEs that have been authenticated are allowed to use the emergency bearer service. These UEs may be in a limited service state in that they may be in an area with restricted service or where they are restricted from services. Enabling this option also causes subscription and location validation to be bypassed.
- **full**: Specifies that only UEs that have been authenticated and have successfully passed subscription and location validation are allowed to use the emergency bearer service. Enabling this option indicates that only UEs that are capable of normal attach procedures will be allowed to use the emergency bearer service.
- **imsi**: Specifies that UEs with an International Mobile Subscriber Identity (IMSI) are allowed to use the emergency bearer service regardless of authentication. Even if authentication fails, the UE is granted access.
- **none**: Specifies that all UEs are allowed to use the service. This is the default value for the command.

Usage

Use this command to indicate which UEs can use the emergency bearer service through this profile.

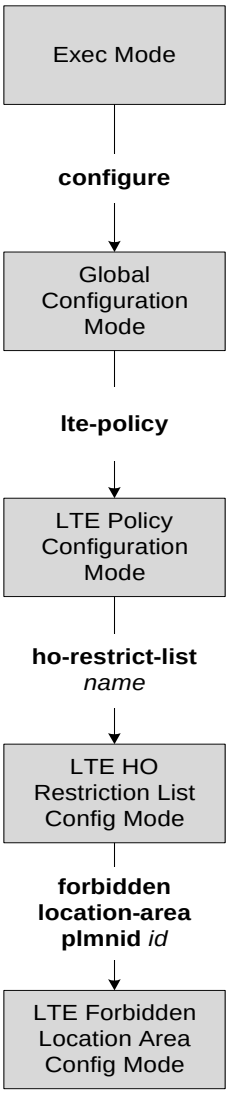
Example

The following command configures the type of UE allowed to use the emergency bearer service to "IMSI required, authentication optional":

```
ue-validation-level imsi
```

Chapter 177
LTE Forbidden Location Area Configuration Mode Commands

The LTE Forbidden Location Area Configuration Mode is used to create and manage forbidden 3G location area code (LAC) configurations.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

lac

Configures a 3G location area code (LAC) or area codes where a UE, associated with this LTE policy, is restricted from participating in a handover scenario.

Product

MME

Privilege

Administrator

Syntax

```
[ no ] lac { area_code } +
```

no

Removes a configured forbidden handover area code or area codes from this policy. If no location area code is specified, then all location area codes are removed.

area_code

Specifies an area code or area codes from which UEs are restricted from participating in a handover as an integer from 0 through 65535. Multiple area codes can be entered (up to 128 in a single line, separated by spaces).

Usage

Use this command to configure 3G location-based area codes that will be forbidden to UEs associated with this LTE policy.

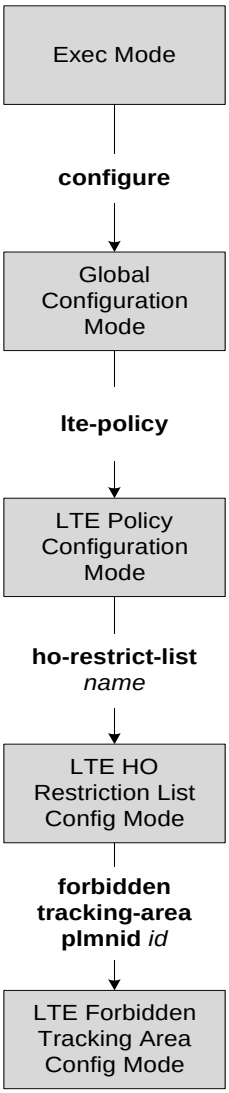
Example

The following command configures eight location-based area codes (1, 2, 3, 4, 5, 6, 7, 8) where a UE, associated with this LTE policy, is restricted from participating in a handover scenario:

```
lac 1 2 3 4 5 6 7 8
```

Chapter 178
LTE Forbidden Tracking Area Configuration Mode Commands

The LTE Forbidden Tracking Area Configuration Mode is used to create and manage forbidden tracking area code (TAC) configurations.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

tac

Configures a tracking area code (TAC) or area codes where a UE, associated with this LTE policy, is restricted from participating in a handover scenario.

Product

MME

Privilege

Administrator

Syntax

[no] tac *area_code*

no

Removes a configured forbidden handover area code or area codes from this policy. If no tracking area code is specified, then all tracking area codes are removed.

area_code

Specifies a tracking area code or area codes from which UEs are restricted from participating in a handover as an integer from 0 to 65535. Multiple area codes can be entered (up to 128 in a single line, separated by spaces).

Usage

Use this command to configure tracking area codes that will be forbidden to UEs associated with this LTE policy.

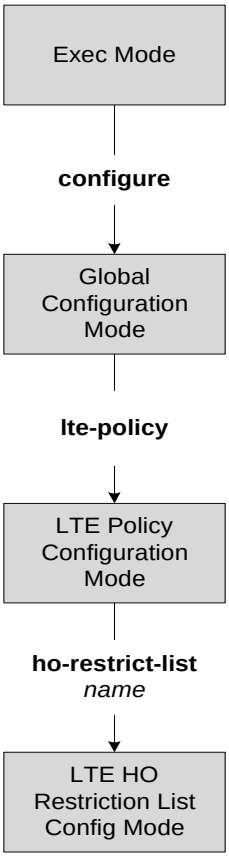
Example

The following command configures two tracking area codes (1, 2, 3, 4, 5, 6, 7, 8) where a UE, associated with this LTE policy, is restricted from participating in a handover *scenario*:

```
tac 1 2 3 4 5 6 7 8
```

Chapter 179
LTE Handover Restriction List Configuration Mode Commands

The LTE Handover Restriction List Configuration Mode is used to create and manage the LTE handover restriction lists for LTE/SAE networks. Handover restriction lists are used to restrict user equipment (UE) from participating in specified handovers. The MME creates the handover restriction lists as part of its local policy and provides them to the eNobeB where the restrictions are enforced.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

forbidden

Configures the handover restriction lists provided to eNodeBs where handover restrictions are enforced for UEs.

Product

MME

Privilege

Administrator

Syntax

```
[ no ] forbidden { inter-rat { all | cdma2000 | geran | utran } | location-area plmnid id
| tracking-area plmnid id }

default forbidden inter-rat
```

default forbidden inter-rat

Removes the forbidden inter-RAT configuration from the LTE policy.

no

Removes the forbidden configuration from the LTE policy.

inter-rat { all | cdma2000 | geran | utran }

Specifies that one or all Radio Access Technology (RAT) handovers are to be prohibited for UEs associated with the LTE policy.
all: Specifies that all inter-RAT handovers are to be prohibited for UEs associated with the LTE policy.
cdma2000: Specifies that all CDMA2000 handovers are to be prohibited for UEs associated with the LTE policy.
geran: Specifies that all GSM EDGE Radio Access Network (GERAN) handovers are to be prohibited for UEs associated with the LTE policy.
utran: Specifies that all UMTS Terrestrial Radio Access Network (UTRAN) handovers are to be prohibited for UEs associated with the LTE policy.

location-area plmnid *id*

Specifies that handovers to 3G location area codes defined through this keyword and subsequent configuration mode are to be prohibited for UEs associated with the LTE policy. Enters the LTE Forbidden Location Area Configuration Mode. *id* must be a valid PLMN ID expressed as an integer comprised of an MCC (Mobile Country Code) and MNC (Mobile Network Code) [five-digit minimum, six-digit maximum].

Important: Up to 16 forbidden location area PLMN IDs can be configured per handover restriction list.

Entering this command results in the following prompt:

```
[context_name]hostname(forbidden_la)#
```

LTE Forbidden Location Area Configuration Mode commands are defined in the *LTE Forbidden Location Area Configuration Mode Commands* chapter.

tracking-area plmnid *id*

Specifies that handovers to 4G tracking area codes defined through this keyword and subsequent configuration mode are to be prohibited for UEs associated with the LTE policy. Enters the LTE Forbidden Tracking Area Configuration Mode. *id* must be a valid PLMN ID and be an integer value comprising an MCC and MNC (five-digit minimum, six-digit maximum).

Important: Up to 16 forbidden tracking area PLMN IDs can be configured per handover restriction list.

Entering this command results in the following prompt:

```
[context_name]hostname(forbidden_ta)#
```

LTE Forbidden Tracking Area Configuration Mode commands are defined in the *LTE Forbidden Tracking Area Configuration Mode Commands* chapter.

Usage

Use this command to create the list of restricted handover types that apply to all UEs associated with the LTE policy.

Example

The following command prohibits UEs associated with this LTE policy from participating in a handover to a GERAN network type:

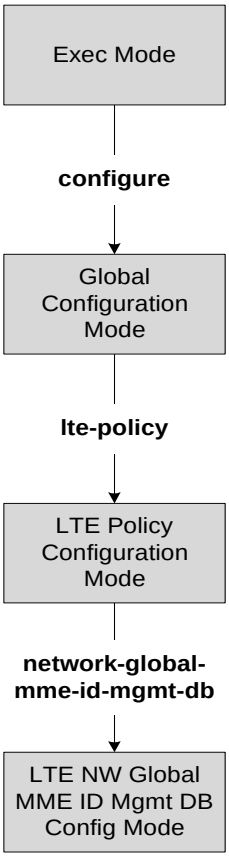
```
forbidden inter-rat geran
```

The following command prohibits UEs, associated with this LTE policy and a mobile network with a PLMN ID of *12345*, from participating in a handover to location area codes defined in the Location Area Configuration Mode:

```
forbidden location-area plmnid 12345
```

Chapter 180
LTE Network Global MME ID Management Database Configuration Mode Commands

The LTE Network Global MME ID Management Database Configuration Mode is used to create associations between PLMN IDs and MME group ID ranges.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

plmn

Configures associations between public land mobile network (PLMN) IDs and ranges of MME group IDs.

Product

MME

Privilege

Administrator

Syntax

[no] plmn mcc *mcc_value* **mnc** *mnc_value* **mme-group-id-range first** *id* **last** *id*

no

Removes the selected PLMN ID to MME group ID range from the MME ID management database.

mcc *mcc_value* **mnc** *mnc_value*

mcc *mcc_value*: Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.
mnc *mnc_value*: Specifies the mobile network code (MNC) portion of the PLMN identifier a 2- or 3-digit integer from 00 through 999.

mme-group-id-range first *id* **last** *id*

Specifies the range of MME group IDs to apply to the PLMN ID as an integer from 0 to 65535.

Usage

Use this command to create associations between PLMN IDs and a range of MME group IDs.

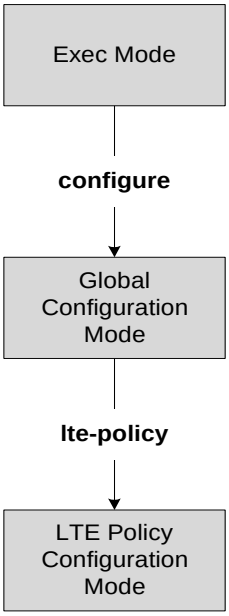
Example

The following command creates an association between a PLMN ID of *12323* and a set of MME group IDs with a range of *500* through *575*:

```
plmn mcc 12323 mnc 23 mme-group-id-range first 500 last 575
```

Chapter 181
LTE Policy Configuration Mode Commands

The LTE Policy Configuration Mode is used to create and manage the LTE policies supporting MME and S-GW configurations on the system.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

ho-restrict-list

Creates a handover (HO) restriction list or specifies an existing HO restriction list and enters the Handover Restriction List Configuration Mode.

Product

MME, S-GW

Privilege

Administrator

Syntax

[no] ho-restrict-list *list_name* **[-noconfirm]**

no

Removes the specified restriction list from the system.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

list_name

Specifies the name of the HO restriction list. If the entered list name does not refer to an existing list, a new list is created. *list_name* is an alphanumeric string of 1 through 64 characters.

Usage

Use this command to enter the Handover Restriction List Configuration Mode for an existing list or for a newly defined list. This command is also used to remove an existing list.
Entering this command results in the following prompt:

```
[context_name]hostname(ho-restrict-list)#
```

Handover Restriction List Configuration Mode commands are defined in the *LTE Handover Restriction List Configuration Mode Commands* chapter.

Example

The following command enters the Handover Restriction List Configuration Mode for a new or existing list named *ho_restricit_list1*:

```
ho-restrict-list ho_restrict_list1
```

lte-emergency-profile

Creates an LTE emergency profile or specifies an existing emergency profile and enters the LTE Emergency Profile Configuration Mode.

Product

MME, S-GW

Privilege

Administrator

Syntax

`[ no ] lte-emergency-profile` *`profile_name`* **`[ -noconfirm ]`**

`no`

Removes an LTE emergency profile from the system.

`name`

Specifies the name of the LTE emergency profile being created or accessed. If the profile name does not refer to an existing profile, a new profile is created. *`profile_name`* is an alphanumeric string of 1 through 64 characters.

`-noconfirm`

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to enter the LTE Emergency Profile Configuration Mode for an existing profile or for a newly defined profile. This command is also used to remove an existing profile.

Important: A maximum of four LTE emergency profiles are allowed per system.

Entering this command results in the following prompt:

```
[context_name]hostname(lte-emergency-profile)#
```

LTE Emergency Profile Configuration Mode commands are defined in the *LTE Emergency Profile Configuration Mode Commands* chapter.

Example

The following command enters the LTE Emergency Profile Configuration Mode for a new or existing profile named *`emergency_profile3`*:

```
lte-emergency-profile emergency_profile3
```

network-global-mme-id-mgmt-db

Creates a new, or enters the existing MME group ID management database.

Product

MME, S-GW

Privilege

Administrator

Syntax

```
[ no ] network-global-mme-id-mgmt-db
```

no

Remove the global MME ID management database from the system.

Usage

Use this command to create a new, or enter the existing MME group ID management database. The MME group ID management database is used to create associations between PLMN IDs and ranges of MME group IDs.

Important: Only one MME group ID management database can be created per system.

Entering this command results in the following prompt:

```
[context_name]hostname(network-global-mme-id-mgmt-db)#
```

Global MME ID management database commands are defined in the *LTE Network Global MME ID Management Database Configuration Mode Commands* chapter.

subscriber-map

Creates a subscriber map or specifies an existing subscriber map and enters the Subscriber Map Configuration Mode.

Product

MME, S-GW

Privilege

Administrator

Syntax

[no] subscriber-map *map_name* **[-noconfirm]**

no

Removes the specified subscriber map from the system.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

map_name

Specifies the name of the subscriber map. If the map name does not refer to an existing map, a new map is created. *map_name* must be an alphanumeric string of 1 through 64 characters.

Usage

Enter the Subscriber Map Configuration Mode for an existing or newly defined map. This command is also used to remove an existing map.
Entering this command results in the following prompt:

```
[context_name]hostname(subscriber-map)#
```

Subscriber Map Configuration Mode commands are defined in the *Subscriber Map Configuration Mode Commands* chapter.

Example

The following command enters the existing Subscriber Map Configuration Mode (or creates it if it does not already exist) for the map named *map1*:

```
subscriber-map map1
```

tai-mgmt-db

Creates a Tracking Area Identifier (TAI) Management Database or specifies an existing database and enters the TAI Management Database Configuration mode.

Product

MME, S-GW

Privilege

Administrator

Syntax

[no] tai-mgmt-db *db_name* **[-noconfirm]**

no

Removes the specified management database from the system.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

db_name

Specifies the name of the management database. If the name does not refer to an existing database, a new database is created. *db_name* is an alphanumeric string of 1 through 64 characters.

Usage

Enter the TAI Management Database Configuration Mode for an existing or newly defined database. This command is also used to remove an existing database.
Entering this command results in the following prompt:

```
[context_name]hostname(tai-mgmt-db)#
```

TAI Management Database Configuration Mode commands are defined in the *TAI Management Database Configuration Mode Commands* chapter.

Example

The following command enters the existing TAI Management Database configuration mode (or creates it if it does not already exist) for the database named *tai_db1*:

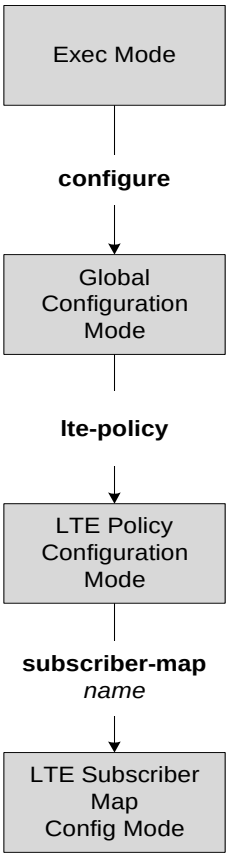
```
tai-mgmt-db tai_db1
```

Chapter 182
LTE Subscriber Map Configuration Mode Commands

The LTE Subscriber Map Configuration Mode is used to create and manage subscriber maps for applying operator policy templates to individual subscribers and/or groups of subscribers.

Subscriber mappings are ordered lists containing explicit UE matching criteria. The maps are examined for specific UE identity information such as the UE's IMSI. The system uses the first map that matches the criteria to associate an operator policy with the UE.

Subscriber maps can be modified but will only affect future subscribers and not subscribers already attached to UEs.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

precedence

Sets the order of precedence, the matching criteria and the association to an operator policy for subscribers meeting the match criteria.

Product

MME, S-GW

Privilege

Administrator

Syntax

precedence *number* **match-criteria all operator-policy-name** *policy_name*

precedence *number* **match-criteria imsi mcc** *mcc_num* **mnc** *mnc_num* **[msin first** *start_range* **last** *end_range* **| service-plmnid** *id* **] operator-policy-name** *policy_name*

precedence *number* **match-criteria service-plmnid** *id* **operator-policy-name** *policy_name*

no precedence *number*

no

Removes the selected precedence number from the subscriber map. *number* must be an integer value from 1 to 1024.

number

Specifies the order of precedence for the subscriber map. 1 is the highest precedence. *number* must be an integer value from 1 to 1024.

match-criteria

Specifies that the keyword following this keyword is the criteria to be used to match a UE.

all

Specifies that all UEs are to be associated with the operator policy.

imsi mcc *mcc_num* **mnc** *mnc_num* **[msin first** *start_range* **last** *end_range* **| service-plmnid** *id* **]**

Specifies that UEs with criteria matching the International Mobile Subscriber Identifier (IMSI) information (MCC and MNC) are to be associated with a specified operator policy.
mcc *mcc_num*: Specifies the mobile country code (MCC) portion of the IMSI identifier as an integer value between 100 and 999.
mnc *mnc_num*: Specifies the mobile network code (MNC) portion of the IMSI identifier as a 2- or 3-digit integer value between 00 and 999.
msin first *start_range* **last** *end_range*: Optionally specifies a range of Mobile Subscriber Identification Numbers that further narrows the match criteria for the IMSI match configuration. *start_range* and *end_range* must each be an integer value of 10 digits.

service-plmnid *id*: Optionally specifies a local service PLMN ID number used further narrow the IMSI-based operator policy selection. *id* must be an integer value of five digits minimum and six digits maximum (the combination of the MCC and MNC).

service-plmnid *id*

Specifies a local service PLMN ID number used for PLMN ID-based operator policy selection. *id* must be an integer value of five digits minimum and six digits maximum (the combination of the MCC and MNC).

operator-policy-name *policy_name*

Sets the operator policy with which the matching criteria is associated. *policy_name* must be an existing operator policy expressed as an alphanumeric string of 1 through 64 characters. Operator policies are configured in the Operator Policy Configuration Mode. For more information about operator policies, refer to the *Operator Policy Configuration Mode Commands* chapter.

Usage

The operator policy provides mechanisms to fine tune the behavior of subsets of subscribers above and beyond the behaviors described in the user profile. It is also used to control the behavior or visiting subscribers in roaming scenarios, enforce roaming agreements, and provide a measure of local protection against foreign subscribers.

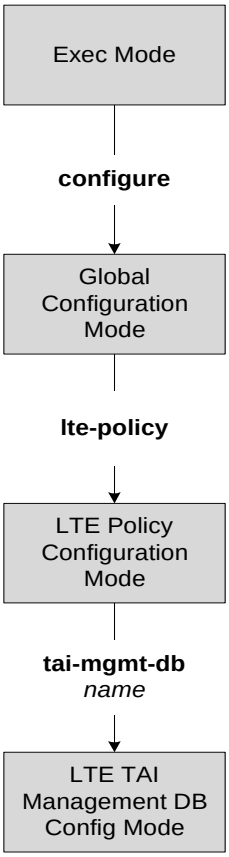
Example

The following command associates the operator policy named *op_pol1* with UEs associated with an IMSI MCC of *111*, an MNC of *222*, and a service PLMN ID of *123456*:

```
precedence 100 match-criteria imsi mcc 111 mnc 222 service-plmnid 123456
operator-policy-name op_pol1
```

Chapter 183
LTE TAI Management Database Configuration Mode Commands

The LTE TAI Management Database Configuration Mode is used to create and manage the LTE Tracking Area Identifier (TAI) management database configuration for LTE polices configured on this system.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

tai-mgmt-obj

Creates new, or removes/enters existing, LTE Tracking Area Identifier (TAI) object configurations.

Product

MME

Privilege

Administrator

Syntax

[no] tai-mgmt-obj *object_name* **[-noconfirm]**

no

Removes a configured TAI management object from the TAI management database.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

object_name

Specifies the name of the TAI management object and enters the LTE TAI Management Object Configuration Mode as an alphanumeric string of 1 through 64 characters.

Usage

Use this command to enter the LTE TAI Management Object Configuration Mode for an existing object or for a newly defined object. This command is also used to remove an existing object.
Entering this command results in the following prompt:

```
[context_name]hostname(tai-mgmt-obj)#
```

LTE TAI Management Object Configuration Mode commands are defined in the *LTE TAI Management Object Configuration Mode Commands* chapter.

Example

The following command creates a TAI management object called *tai-obj3* and enters the LTE TAI Management Object Configuration Mode:

```
tai-mgmt-obj tai-obj3
```

timezone

Configures the timezone to be used for the UE timezone in S11 and Non Access Stratum (NAS) messages.

Product

MME

Privilege

Administrator

Syntax

timezone { + | - } hours *value* **[minutes { 0 | 15 | 30 | 45 }]**

no timezone

Removes the timezone configuration from the management database.

+ | -

Specifies the offset direction from the Coordinated Universal Time (UTC).

hours *value*

Specifies the offset from UTC in hours. *value* must be an integer from 0 through 14.

minutes { 0 | 15 | 30 | 45 }

Optionally specifies the offset minutes added to the hours value.

Usage

Use this command to configure the timezone to be used for the UE timezone in S11 and NAS messages.

Important: Time zone configurations at the TAI Management Object level take precedence over time zone configurations at the TAI Management Database level. If neither is configured, the system defaults to the MME time zone.

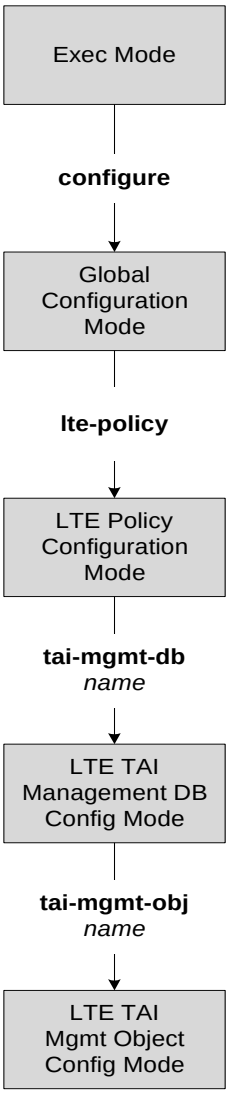
Example

The following command sets the timezone mapping for this management database to plus-3 hours and 15 minutes from UTC:

```
timezone + hours 3 minutes 15
```

Chapter 184
LTE TAI Management Object Configuration Mode Commands

The LTE TAI Management Object Configuration Mode is used to create and manage the LTE Tracking Area Identifiers for the TAI database.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

lai

Configures a Location Area Identifier (LAI) for this TAI management object.

Product

MME

Privilege

Administrator

Syntax

lai mcc *number* **mnc** *number* **lac** *area_code*

no lai

no

Removes a configured LAI from the TAI management object.

mcc *number*

Specifies the mobile country code (MCC) portion of a PLMN identifier as an integer from 100 through 999.

mnc *number*

Specifies the mobile network code (MNC) portion of a PLMN identifier as a 2- or 3-digit integer from 00 through 999.

lac *area_code*

Specifies the Location Area Code portion of the TAI as an integer from 1 through 65535.

Usage

Use this command to configure an LAI for this management object.

Example

The following command adds an LAI to this management object with an MCC of *111*, an MNC of *22*, and a LAC of *101*:

```
lai mcc 122 mnc 22 lac 101
```

sgw-address

Configures an IP address for a Serving Gateway (S-GW), a supported S5/S8 protocol type, and selection weight used in a pool for S-GW selection.

Product

MME

Privilege

Administrator

Syntax

sgw-address *ipv4_or_ipv6_address* **s5-s8-protocol { both | gtp | pmip } weight** *number*

no sgw-address *ipv4_or_ipv6_address* **s5-s8-protocol { both | gtp | pmip }**

no sgw-address *ipv4_or_ipv6_address* **s5-s8-protocol { both | gtp | pmip }**

Removes the configured S-GW address from this TAI management object.

ipv4_or_ipv6_address

Specifies the IP address of the S-GW in the selection pool in IPv4 dotted-decimal or IPv6 colon-separated notation.
Up to 32 S-GW addresses can be configured per TAI management object.

s5-s8-protocol { both | gtp | pmip }

Specifies the S5/S8 interface type found between the configured S-GW and the P-GW.
both: Specifies that both the GTP and PMIP protocols are supported over the S5/S8 interface.
gtp: Specifies that the GTP protocol is supported over the S5/S8 interface.
pmip: Specifies that the PMIP protocol is supported over the S5/S8 interface.

weight *number*

Specifies the priority or weight of the S-GW address used during weighted round-robin selection within this TAI management object. *number* must be an integer from 1 through 100.

Usage

Use this command to configure a pool of S-GW addresses used for S-GW selection.

Example

The following command configures an S-GW with an IPv4 address of *10.2.3.4*, a supported S5/S8 protocol type of GTP, and a selection weight of *3*:

```
sgw-address 10.2.3.4 s5-s8-protocol gtp weight 3
```

tai

Configures a Tracking Area Identifier (TAI) for this TAI management object.

Product

MME

Privilege

Administrator

Syntax

[no] tai mcc *number* **mnc** *number* **{ tac** *value* **} +**

no

Removes a configured TAI from the TAI management object.

mcc *number*

Specifies the mobile country code (MCC) portion of a PLMN identifier as an integer from 100 through 999.

mnc *number*

Specifies the mobile network code (MNC) portion of a PLMN identifier as a 2- or 3-digit integer from 00 through 999.

tac *value* **+**

Specifies the Tracking Area Code portion of the TAI as an integer from 1 through 65535. Up to 16 TAC values can be entered on a single line.

Usage

Use this command to configure one or more TAIs for this management object. Up to 16 TAIs can be configured per management object.

Example

The following command adds a TAI to this management object with an MCC of *111*, an MNC of *22*, and a TAC value of *1001*:

```
tai mcc 122 mnc 22 tac 1001
```

timezone

Configures the timezone to be used for the UE timezone in S11 and Non-Access Stratum (NAS) messages.

Product

MME

Privilege

Administrator

Syntax

timezone { + | - } hours *value* **[minutes { 0 | 15 | 30 | 45 }]**

no timezone

Removes the timezone configuration from the management object.

+ | -

Specifies the offset direction from Coordinated Universal Time (UTC).

hours *value*

Specifies the offset from UTC in hours as an integer from 0 through 14.

minutes { 0 | 15 | 30 | 45 }

Optionally specifies the offset minutes added to the hours value.

Usage

Use this command to configure the time one to be used for the UE timezone in S11 and NAS messages.

Important: Time zone configurations at the TAI Management Object level take precedence over time zone configurations at the TAI Management Database level. If neither is configured, the system defaults to the MME time zone.

Example

The following command sets the time zone mapping for this management object to plus-3 hours and 15 minutes from UTC:

```
timezone + hours 3 minutes 15
```

zone-code

Configures a zone code for the management object.

Product

MME

Privilege

Administrator

Syntax

zone-code *zc_id*

no zone-code

no

Removes the configured zone-code from the management object.

zc_id

Identifies the zone code configuration instance as an integer from 1 through 65535.

Usage

Important: While there is no limit to the number of zone codes that can be created, only 10 LACs per zone code can be defined.

Use this command to define zone code restrictions. Regional subscription data at the home subscriber service (HSS) is used to determine the regional subscription area in which the subscriber is allowed to roam. The regional subscription data consists of a list of zone codes which are comprised of one or more location areas (identified by a LAC) into which the subscriber is allowed to roam. Regional subscription data, if present in the Insert-Subscriber-Data-Request (IDR) and the Update-Location-Answer (ULA) from the HSS, defines the subscriber's subscription area for the addressed MME. It contains the complete list (up to 10 zone codes) that apply to a subscriber in the currently visited PLMN. During the Location Update procedure, the zone code list is received in the ULA from the HSS. The zone code list is validated against the configured values in this command. If matched, the Location Update procedure is allowed to proceed. If not matched, the response is that the Network Node Area is restricted and the Location Update procedure fails.

Example

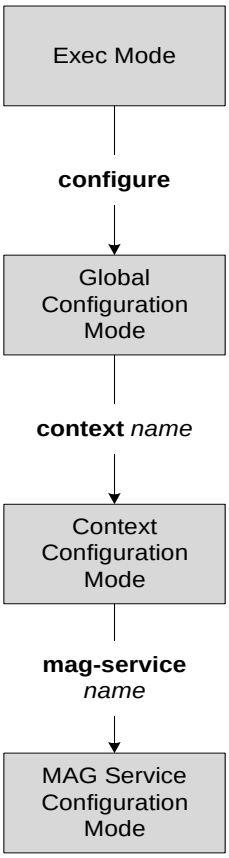
The following command sets the zone code for this management object to *1*:

```
zone-code 1
```

Chapter 185
MAG Service Configuration Mode Commands

Products using commands in this mode: HSGW, S-GW

The MAG Service Configuration Mode is used to create and manage a Mobility Access Gateway service in an HSGW (eHRPD network) or a P-MIP S-GW (LTE-SAE network). The MAG is the PMIP client and communicates with the Local Mobility Anchor (LMA) configured on a PDN Gateway (P-GW).



bind address

Binds the service to a logical IP interface serving as the S2a (HSGW) or S5/S8 (S-GW) interface and specifies the maximum number of subscribers that can access this service over the configured interface.

Product

HSGW, S-GW

Privilege

Administrator

Syntax

bind address *ip_address* **[max-subscribers** *num* **]**

no bind address

no

Removes the interface binding from this service.

ip_address

Specifies the IPv6 address of the interface configured as the S5/S8 interface. *ip_address* is specified in IPv6 colon-separated notation.

max-subscribers *num*

Default: 1500000
Specifies the maximum number of subscribers that can access this service on this interface. *num* must be an integer from 0 through 3000000.

Important: The maximum number of subscribers supported depends on the installed license key and the number of active packet processing cards in the system. A fully loaded system can support 3,000,000 total subscribers. Refer to the **license key** command and the *Usage* section (below) for additional information.

Usage

Associate the MAG service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an S2a or S5/S8 interface that provides the session connectivity to/from a P-GW. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.
This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.
When configuring the **max-subscribers** option, be sure to consider the following:

- The total number of S2a or S5/S8 interfaces you will configure
- The total number of subscriber sessions that all of the configured interfaces may handle during peak busy hours
- An average bandwidth per session multiplied by the total number of sessions
- The type of physical port to which these interfaces will be bound

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

Example

The following command would bind the logical IP interface with the address of *4551:0db8:85a3:08d3:3319:8a2e:0370:1344* to the MAG service and specifies that a maximum of *300,000* simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 4551:0db8:85a3:08d3:3319:8a2e:0370:1344 max-subscribers
300000
```

encapsulation

Configures data encapsulation type to be used for specific MAG service.

Product

HSGW, S-GW

Privilege

Administrator

Syntax

```
encapsulation { gre | ipip }

default encapsulation
```

default

Resets the encapsulation type to be used by this service to the default option of GRE.

{ gre | ipip }

gre: Specifies that GRE encapsulation is to be used for PMIPv6 tunnel data between the MAG and the Local Mobility Anchor (LMA). This is the default for this command.
ipip: Specifies that IP-in-IP encapsulation is to be used for PMIPv6 tunnel data between the MAG and the LMA.

Usage

Use this command to select the encapsulation type to be used for PMIPv6 tunnel data between the MAG and the LMA.

Example

The following command sets the encapsulation data to IP-in-IP:

```
encapsulation ipip
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

information-element-set

Identifies the information element set of mobility options to be used in Proxy Binding Update (PBU) messages sent by the MAG to the LMA.

Product

HSGW, S-GW

Privilege

Administrator

Syntax

```
information-element-set { custom1 | standard }

default information-element-set
```

default

Resets the command to the default value of "standard".

{ custom1 | standard }

custom1: Specifies that a custom set of mobility options will be used in proxy binding update messages that are sent in Vendor Specific Mobility Options. These options are:

- User Location Info
- Hardware Identifier
- Access Network Charging Identifier

standard: Specifies that a standard set of mobility options are to be used in proxy binding update messages. 3GPP specification 29.275 defines these as Protocol Configuration Options.

Usage

Use this command to identify the type of information element set of mobility options to be used in PBU messages sent form the MAG to the LMA. The mobility options can be either standards-based (3GPP 29.275) or custom (vendor-specific as defined by 3GPP 29.275).

Example

The following command identifies the information element set of mobility options to use in PBU messages as custom:

```
information-element-set custom1
```

max-retransmissions

Configures maximum number of retransmissions of Proxy MIP control messages to the Local Mobility Anchor (LMA).

Product

HSGW, S-GW

Privilege

Administrator

Syntax

max-retransmissions *num*

default max-retransmissions

default

Rests the maximum number of allowed retransmissions to the default value of 5.

num

Default: 5
Specifies the maximum number of times the MAG service will attempt to communicate with the LMA before it marks it as unreachable.
count must be an integer from 1 through 4294967295.

Usage

Use this command to limit the number of retransmissions to LMA before marking it as unreachable. If the value configured is reached, the call is dropped.

Example

The following command configures the maximum number of retransmissions for the MAG service to *3*:

```
max-retransmissions 3
```

mobility-option-type-value

Changes the mobility option type value used in mobility messages.

Product

HSGW, S-GW

Privilege

Administrator

Syntax

```
mobility-option-type-value { custom1 | standard }

default mobility-option-type-value
```

default

Sets the command to the default value of custom1.

custom1

(Default) Non-standard type values used before they were defined by IANA.

standard

Standard type values as defined by IANA. In addition, standard option uses type values defined in RFC 5844 for home address (HoA) options for the PMIPv6 PBU/PBA/revocation message.

Usage

Use this command to change the mobility option type value used in mobility messages.

Example

The following command changes the mobility option type value to standard:

```
mobility-option-type-value standard
```

reg-lifetime

Configures the Mobile IPv6 session registration lifetime for this service.

Product

HSGW, S-GW

Privilege

Administrator

Syntax

reg-lifetime *seconds*

default reg-lifetime

default

Resets the command value to the default setting of 600.

seconds

Default: 600
Sets the time value (in seconds) for session lifetimes for this service.
seconds must be an integer from1 through 262140.

Usage

Use this command to limit PMIPv6 lifetime on this service. If the Proxy Binding Acknowledge (PBA) from the LMA contains a lifetime shorter or longer than what is specified, it is used instead.

Example

The following command sets the registration lifetime for Mobile IPv6 sessions using this service to *1200* seconds (20 minutes):

```
reg-lifetime 1200
```

renew-percent-time

Configures percentage of lifetime at which a registration renewal is sent to the Local Mobility Anchor (LMA).

Product

HSGW, S-GW

Privilege

Administrator

Syntax

renew-percent-time *percent*

default renew-percent-time

default

Resets the command to the default value of 75.

percent

Default: 75
Specifies the time percentage when the registration renewal is sent to the LMA. *percent* is a percentage value of the registration lifetime expressed as an integer from 1 through 100.

Usage

Use this command to specify when a registration renewal is sent to the LMA for subscribers using this service.
If the registration lifetime is 600 seconds (10 minutes) and this command is set to 75 (percent), then the registration renewal message is sent after 450 seconds of the registration lifetime has expired.

Example

The following command sets the registration renewal time for subscribers using this service to *90* percent of the registration lifetime:

```
renew-percent-time 90
```

retransmission-policy

Configures the retransmission policy for Proxy MIP control message retransmissions.

Product

HSGW

Privilege

Administrator

Syntax

```
retransmission-policy { exponential-backoff | normal }

default retransmission-policy
```

default

Returns the command to its default setting of exponential-backoff.

{ exponential-backoff | normal }

Sets the retransmission timeout behavior for this service.
exponential-backoff: Specifies that the Proxy Binding Update (PBU) retransmission uses an exponential backoff to increase the retransmission timeout for each retry.
normal: Specifies that the PBU retransmission uses the configured retransmission timeout value for all PBU retransmission retries.

Usage

Use this command to specify the retransmission policy for PMIP control messages.

Example

The following command sets the retransmission timeout policy for PMIP control packets to “normal”:

```
retransmission-policy normal
```

retransmission-timeout

Configures the maximum allowable time for the MAG service to wait for a response from the LMA before it attempts to communicate with the LMA again (if the system is configured to retry the LMA), or marks the LMA as unreachable.

Product

HSGW, S-GW

Privilege

Administrator

Syntax

retransmission-timeout *time*

[default | no] retransmission-timeout

default

Resets the timeout setting to the default value of 3,000 milliseconds.

no

Deletes a previously configured timeout value.

time

Default: 3000
Specifies the maximum allowable time (in milliseconds) for the MAG service to wait for a response from the LMA before it: (a) attempts to communicate with the LMA again (if the system is configured to retry the LMA) or (b) marks the LMA as unreachable.
time must be an integer from 100 through 100000.

Usage

Use the retransmission timeout command in conjunction with the **max-retransmissions** command in order to configure the MAG services behavior when it does not receive a response from a particular LMA.

Example

The following command configures a retransmission timeout value of 5000 milliseconds:

```
retransmission-timeout 5000
```

signalling-packets

Enables the QoS Differentiated Services Code Point (DSCP) marking feature for IP headers carrying outgoing signalling packets.

Product

HSGW, S-GW

Privilege

Administrator

Syntax

signalling-packets ip-header-dscp *value*

[default | no] signalling-packets ip-header-dscp

default

Restores the specified parameter to its default setting of 0x0.

no

Disables the specified functionality.

ip-header-dscp *value*

Used to configure the QoS Differentiated Services Code Point (DSCP) marking for IP header encapsulation. *value*: Represents the DSCP setting as the first six most-significant bits of the ToS field. It can be configured to any hexadecimal value from 0x0 through 0x3F. Default is 0x0.

Usage

Use this command to enable or disable the DSCP marking feature for IP headers carrying outgoing signalling packets. DSCP marking is disabled by default.

Example

The following command configures the HSGW service to support DSCP marking for IP headers carrying outgoing signalling packets:

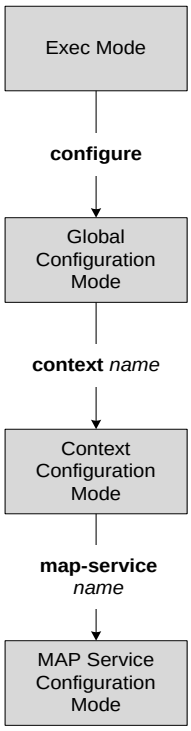
```
signalling-packets ip-header-dscp 0x21
```

Chapter 186
MAP Service Configuration Mode Commands

The MAP Service Configuration Mode is used to configure properties for Mobile Application Part (MAP) service.

Mobile Application Part (MAP) is a protocol which provides an application layer for the various nodes in the core mobile network and GPRS and UMTS core network to communicate with each other in order to provide services to mobile phone users. The MAP service provides the application-layer protocol support used to access the Home Location Register (HLR).

[<*context_name*>]*hostname*(config-map-service-<*svc_name*>)#



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

access-protocol

Configures access protocol parameters for the MAP service as defined for a specific SCCP network instance.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

access-protocol sccp-network *sccp_id* **ssn** *subsys_num*

no access-protocol sccp-network *sccp_id* **ssn** *subsys_num*

sccp-network *sccp_id*

Specifies the ID number of the SCCP network to use for the SGSN connection.
sccp_id : Must be an integer from 1 to 16.

ssn *subsys_num*

Identifies the subsystem number for the destination.
subsys_num: Enter an integer from 1 through 255.

no

Removes the access protocol SCCP network instance ID from the configuration.

Usage

Use this command to associate access protocol parameters to a specific instance of the MAP service for an SCCP network.

Example

The following command associates the access protocols with the SCCP network ID #10:

```
access-protocol sccp-network 10
```

application-context-name

Configure the operation timer(s) for one or more MAP application contexts.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

application-context-name *application* **operation-timer** *value*

default application-context-name *application* **operation-timer**

default

Resets the operation timers for all applications to system defaults.

application

Select one of the following applications to enable the application:

- **authentication-failure-report** : Sets the reporting operation timer for authentication failure. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **cancel-location** : Sets the cancel location operation timer. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **check-imei** : Sets the check-IMEI operation timer. The setting range for this timer is 15 to 30 seconds for releases 8.0 and 8.1 and 1 to 30 seconds for releases 9.0 and higher. The default setting is 15 seconds.
- **delete-subscriber-data** : Sets the delete subscriber data operation timer. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **mo-fwd-sm** : Sets the operation timer for fowarding mobile-originated SMS. The setting range for this timer is 1 to 10 minutes and the default setting is 1 minute (60 seconds).
- **ms-purge** : Sets the operation timer for MS-purge function. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **mt-fwd-sm** : Sets the operation timer for fowarding mobile-terminated SMS. The setting range for this timer is 1 to 10 minutes and the default setting is 1 minute (60 seconds).
- **ready-for-sm** : Sets the operation timer for the ready for SMS operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **send-authentication-info** : Sets the operation timer for the sending authentication information operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **stand-alone-insert-subscriber-data** : Sets the operation timer for the standalone insert subscriber data operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **ugl-insert-subscriber-data** : Sets the operation timer for the insert subscriber data portion of the update GPRS location operation. TThe setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.

- **update-gprs-location** : Sets the operation timer for the update GPRS location operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.

operation-timer*value*

Configures the operation timer for the selected application. Timer values are indicated above.

Usage

Repeat this command entering a different application each time to enable multiple applications.

Example

application-context-name *stand-alone-insert-subscriber-data operation-timer* **operation-timer** *20*

auth-vectors

Configures the number of authorization vectors to be requested from the home location register (HLR) during call setup to provide subscriber authentication.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

auth-vectors number-to-request *number*

default auth-vectors number-to-request

default

Resets the number of vectors requested from the HLR to the system default.

number-to-request *number*

number: Must be an integer from 1 to 5 to define the number of authorization vectors be requested from the HLR.
Default is 5.

Usage

Set the number of requests to be received from the HLR.

Example

auth-vectors number-to-request *4*

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

equipment-identity-register

Defines the information relevant to the equipment-identity-register (EIR) used by the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

equipment-identity-register { isdn *E.164_num* **| point code** *pt_code* **} [source-ssn** *ssn***| check-imei-every-n-events***times*]

no equipment-identity-register { isdn *E.164_num* **| point code***pt_code* **}**

no

Deletes the EIR configuration.

isdn *number*

Enter the E.164 number of the EIR.
number: must be a string of 1 to 15 digits.

point code *pt_code*

Enter SS7 point code address of the EIR in dotted-decimal format according to variant settings:

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- or a string of 1 to 11 characters

source-ssn *ssn*

Identifies the subsystem number (SSN) to be used.
ssn must be an integer from 1 to 255.

check-imei-every-n-events *times*

Configures the frequency with which a 'check IMEI' message is sent to the EIR. When set, the SGSN skips sending the 'check IMEI' message for the first N-1 where IMDI/IMEISV is received.
times :

- For releases 8.0 and 8.1, the value must be an integer from 1 to 15.
- For releases 9.0 and higher, the value must be an integer from 1 to 255.

Important: This feature requires the enabling of **verify-equipment-identity** for IMEI or IMEISV as specified with the the **gmm retrieve-equipment-identity imei** command of the call-control-profile configuration mode.

Usage

Configure the identity of the EIR that the SGSN uses and the interaction parameters.
Increasing the **check-imei-every-n-events** frequency enables the EIR to avoid overload as the number of data-only devices attaching to the network increases.

Example

Configure EIR with point code 1.255.1 to perform IMEI check after every 61st received Attach Request message:

```
equipment-identity-register point code 1.255.1 check-imei-every-n-events
62
```

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

hlr

This command enters the configuration mode for the home location register (HLR). The HLR is a database containing the subscriber profile information for all mobile stations (MS) / user equipment (UE) connecting to a specific GPRS or UMTS core network.

Important: The commands and options for this mode are documented in the HLR Configuration Mode chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
hlr
```

policy

This command configures the Transaction Capabilities Application Part (TCAP) -specific MAP policy for either ANSI or ITU SS7 variants.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default ] policy tcap { use-received-destination-address | use-received-source-address
}
```

use-received-destination-address

Selecting this keyword overwrites stored CG and CD addresses with a new address received in first TC CNT msg

use-received-source-address

Selecting this keyword instructs the MAP service to use the received source address for the dialog.

Usage

Use this command to determine how TCAP will handle MAP messages.

Example

```
policy tcap use-received-destination-address
```

short-message-service

This command enables and disables the short message service (SMS service) and provides access to the SMS Service configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
short-message-service
```

```
no short-message-service
```

no

Disables the SMS service.

Usage

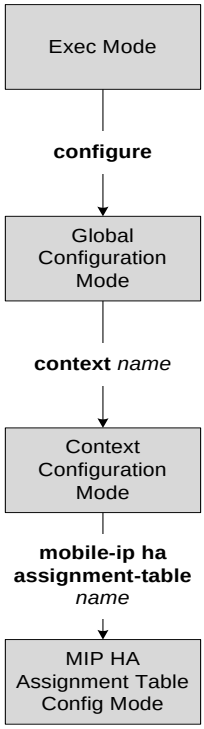
Enter the command to access the SMS service configuration mode to fine tune the SMS functionality.

Example

```
short-message-service
```

Chapter 187
MIP HA Assignment Table Configuration Mode Commands

The Mobile IP HA Assignment Table Configuration Mode is used to assign specific Home Agent (HA) IP addresses to ranges of Mobile Node (MN) IP addresses.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

hoa-range

This command assigns ranges of Mobile Node (MN) IP addresses to specific Home agent IP addresses.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

hoa-range *ip_addressip_address2* **ha** *ip_address3*

no hoa-range *ip_address ip_address2 ha ip_address3*

no

Removes the specified Home Agent assignment from the assignment table.

ip_address ip_address2

Specifies a range of MN IP addresses. *ip_address* and *ip_address2* must be specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

ha *ip_address3*

Specifies the IP address of the Home Agent to assign to MNs that are within the specified range. *ip_address3* must be specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to assign ranges of MN IP addresses to specific HAs.

Important: A maximum of eight MIP HA assignment tables can be configured per context with a maximum of eight MIP HA assignment tables across all contexts.

Important: A maximum of 256 non-overlapping hoa-ranges can be configured per MIP HA Assignment table with a maximum of 256 non-overlapping hoa-ranges across all MIP HA Assignment tables.

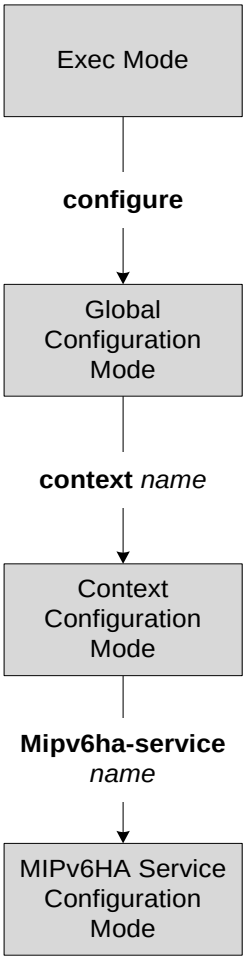
Example

The following command assigns any MN IP address that falls in the range of *192.168.100.0* through *192.168.101.0* to the HA with the IP address of *192.168.200.10*:

```
hoa-range 192.168.100.0 192.168.101.0 ha 192.168.200.10
```

Chapter 188
MIPv6HA Service Configuration Mode Commands

The MIPv6 HA Service Configuration Mode is used to create and manage Mobile IPv6 (MIPv6) access privileges.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

aaa accounting

Configures the sending of subscriber session AAA accounting by the Home Agent (HA) service.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

```
aaa accounting

no aaa accounting
```

Usage

Enabling the HA service will send all accounting data (start, stop, and interim) to the configured AAA servers. The default is AAA accounting enabled.

Important: In order for this command to function properly, AAA accounting must be enabled for the context in which the HA service is configured using the **aaa accounting subscriber radius** command.

Example

AAA accounting for the HA service can be disabled using the **no** version of the command.

The following command disables aaa accounting for the HA service:

```
no aaa accounting
```

bind

Designates the address of the MIPv6HA service and specifies the maximum number of subscribers that can access this service over the interface.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

bind address *IPv6_address* **[max-subscribers** *count* **]**

no bind address

address

Specifies the IPv6 address of the MIPv6HA service using IPv6 colon-separated notation.

max-subscribers *count*

Default: 3000000
Specifies the maximum number of subscribers that can access this service on this interface.
count is an integer from 0 through 4000000.

default

Restore default values assigned for specified parameter.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

```
default { aaa | refresh-advice-option | refresh-interval-percent | reg-lifetime |
sequence-number-validate | setup-timeout | simul-bindings | subscriber | timestamp-
replay-protection }
```

aaa

Restores the AAA setting configured by the **aaa** command to its default of enabled.

refresh-advice-option

Restores the refresh-advice-option setting to its default of disabled.

refresh-interval-percent

Restores the refresh-interval-percent setting to its default of 75.

reg-lifetime

Restores the Mobile IP session registration lifetime setting configured by the **reg-lifetime** command to its default: 600 seconds.

sequence-number-validate

Restores the sequence-number-validate setting to its default of enabled.

setup-timeout

Restore the maximum amount of time allowed for setting up a session to the default: 60 seconds.

simul-bindings

Restores the simultaneous bindings setting to its default: 1.

subscriber

Configures settings for the default subscriber.

timestamp-replay-protection

Restores the timestamp-replay-protection scheme according to RFC 4285.

Usage

After the system has been modified from its default values, this command is used to set or restore specific parameters to their default values.

Example

The following command is used to return the simultaneous bindings setting parameter to it's default value:

```
default simul-bindings
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

refresh-advice-option

Configures inclusion of refresh advice option in the Binding Acknowledgement sent by the Home Agent (HA).

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

```
refresh-advice-option
```

Usage

Includes the refresh advice option in the binding acknowledgements sent by the home agent. Default is disabled.

refresh-interval-percent

Configures the percentage of the granted lifetime to be used in the refresh interval mobility option in the Binding Acknowledgement sent by the Home Agent (HA).

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

refresh-interval-percent *value*

value

value represents a percentage expressed as an integer from 1 through 99. Default is 75.

Usage

Use this command to configure the amount of the granted lifetime to be used in the refresh interval mobility option in the Binding Acknowledgement sent by the Home Agent (HA).

Example

The following command sets the refresh-interval-percent value to 50%:

```
refresh-interval-percent 50
```

reg-lifetime

Specifies the longest registration lifetime that the HA service will be allowed in any Registration Request message from the mobile node.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

reg-lifetime *time*

no

Sets the registration lifetime to infinite.

time

Specifies the registration lifetime in seconds. *time* is an integer from 1 through 262140. Default is 600.

Usage

Use to limit a mobile nodes' lifetime. If the mobile node requests a shorter lifetime than what is specified, it is granted. However, Per RFC 2002, should a mobile node request a lifetime that is longer than the maximum allowed by this parameter, the HA service will respond with the value configured by this command as part of the Registration Reply.

Example

The following command configures the registration lifetime for the HA service to be 2400 seconds:

```
reg-lifetime 2400
```

The following command configures an infinite registration lifetime for MIPv6 calls:

```
no reg-lifetime
```

sequence-number-validate

Configures sequence number validation of the received MIPV6 control packet by the Home Agent (HA) according to RFC 3775.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

```
sequence-number-validate
```

Usage

Use this command to enable sequence number validation of the received MIPV6 control packet by the Home Agent (HA) as per RFC 3775. Default is enabled.

setup-timeout

The maximum amount of time allowed for session setup.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

setup-timeout *seconds*

seconds

Default: 60 seconds
The maximum amount of time (in seconds) to allow for setup of a session expressed as an integer from 1 through 1000000. Default is 60 seconds.

Usage

Use this command to set the maximum amount of time allowed for setting up a session.

Example

To set the maximum time allowed for setting up a session to 5 minutes (300 seconds), enter the following command:

```
setup-timeout 300
```

simul-bindings

Specifies the maximum number of “care-of” addresses that can be simultaneously bound for the same user as identified by NAI and Home address.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

simul-bindings *number*

number

Configures maximum number of "care of" addresses that can be simultaneously bound for the same user as identified by their NAI and home address. *number* is an integer from 1 through 3. Default is 1.

Usage

Per RFC 2002, the HA service creates a mobile binding record (MBR) for each subscriber session it is facilitating. Each MBR is associated with a care-of address. As the mobile node roams, it is possible that the session will be associated with a new care-of address.
Typically, the HA service will delete an old binding and create a new one when the information in the Registration Request changes. However, the mobile could request that the HA maintains previously stored MBRs. This command allows you to configure the maximum number of MBRs that can be stored per subscriber if the requested.

Example

The following command configures the service to support up to *2* addresses per subscriber:

```
simul-bindings 2
```

timestamp-replay-protection tolerance

Designates timestamp replay protection scheme as per RFC 4285.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

timestamp-replay-protection tolerance*seconds*

tolerance *seconds*

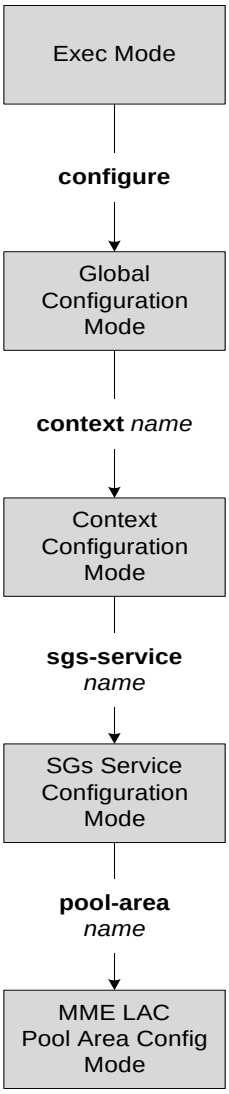
Defines the acceptable difference in timing (between timestamps) before rejecting packet, in seconds. *seconds* must be an integer from 0 through 65535. The default is 7.

Usage

Use this command to define the acceptable difference in timing (between timestamps) before rejecting packet.

Chapter 189
MME LAC Pool Area Configuration Mode Commands

The MME LAC Pool Area Configuration Mode is used to create and manage the Location Area Code (LAC) pool areas.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

hash-value

Configures the Visitor Location Register (VLR) hash value mapping for this pool area.

Product

MME

Privilege

Administrator

Syntax

hash-value { *value* | non-configured-values | range *value* to *value* } use-vlr *vlr_name*

no hash-value { *value* | non-configured-values | range *value* to *value* }

no

Removes the configured hash-value from the pool-area configuration.

value

Specifies the VLR hash value to be used with the configured VLR. *value* must be an integer from 0 through 999.

non-configured-values

Specifies that the VLR configured in this command is to be used non-configured hash values.

range *value* to *value vlr_name*

Specifies a range of hash values to use with the configured VLR as an integer from 0 through 999.

use-vlr

Specifies the VLR to be used with the hash value configuration in this command.

Usage

Use this command to configure hash values to be used with VLRs.
In a pool configuration, the MME selects the VLR that corresponds to the hash of the UE's IMSI. If that VLR is inactive, the MME will use the default VLR (as defined by the **non-configured-value** option). If no default VLR has been configured, or if the default VLR is inactive, the MME selects any other available VLR from the pool.
If the chosen VLR is active at the time of selection and then subsequently becomes inactive when the request is sent to it, the current request fails. On the next request from the UE, the VLR selection mechanism is applied again. A VLR that failed previously will only be selected again if it became active since the earlier failure.

Example

The following command configures all hash values within a range of *0* to *500* to use a VLR named *vlr1*:

```
hash-value range 0 to 500 use-vlr vlr1
```

The following command configures hash values of *501* to use a VLR named *vlr2*:

```
hash-value 501 use-vlr vlr2
```

The following command configures all non-configured hash values to use a VLR named *vlr3*:

```
hash-value non-configured-values use-vlr vlr3
```

lac

Configures a 3G location area code or area codes that define this pool area.

Product

MME

Privilege

Administrator

Syntax

```
[ no ] lac { area_code } +
```

no

Removes a configured forbidden handover area code or area codes from this policy. If no location area code is specified, then all location area codes are removed.

area_code

Specifies an area code or area codes used to select a VLR for the pool area as an integer from 0 through 65535. Multiple area codes can be entered (up to 16 in a single line, separated by spaces).

Important: A total of 16 area codes can be added in a single line or separately.

Usage

Use this command to configure 3G location-based area codes that define this pool area.

Example

The following command configures eight location-based area codes (1, 2, 3, 4, 5, 6, 7, 8) that define this pool area:

```
lac 1 2 3 4 5 6 7 8
```

plmn-id

Configures the Public Land Mobile Network (PLMN) identifier for the LAC pool area. The PLMN identifier is consists of the Mobile Country Code (MCC) and the Mobile Network Code (MNC).

Product

MME

Privilege

Administrator

Syntax

plmn-id mcc *mcc_value* **mnc** *mnc_value*

no plmn-id

no

Removes the configured PLMN identifier for the LAC pool area.

mcc *mcc_value*

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

mnc *mnc_value*

Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

Usage

Use this command to set the PLMN identifier for the LAC pool area.

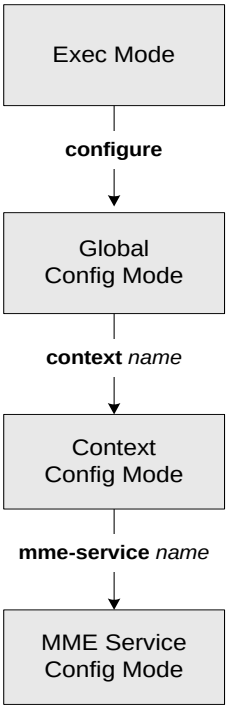
Example

The following command configures the PLMN identifier with MCC value as *102* and MNC value as *20* for this MME service:

```
plmn-id mmc 102 mnc 20
```

Chapter 190
MME Service Configuration Mode Commands

The MME Service Configuration Mode is used to create and manage the LTE Mobility Management Entity (MME) services for the LTE/SAE network. This service works in conjunction with MME-HSS Service and eGTP Service.



associate

Associates or disassociates supportive services and policies, such as an Evolved GPRS Tunnelling Protocol (eGTP) service, an HSS peer service, or an MME policy subscriber map with an MME service.

Product

MME

Privilege

Administrator

Syntax

associate { { egtp-service *egtp_svc_name* **| egtp-sv-service** *egtp_sv_svc_name* **| hss-peer-service** *hss_svc_name* **| lte-emergency-profile** *profile_name* **| network-global-mme-id-mgmt-db | sctp-param-template** *template_name* **| sgs-service** *sgs_svc_name* **| sgtpc-service** *sgtpc_svc_name* **} [context** *ctx_name* **] | subscriber-map** *map_name* **| tai-mgmt-db** *database_name* **}**

no associate { egtp-service | egtp-sv-service | hss-peer-service | lte-emergency-profile | network-global-mme-id-mgmt-db | sctp-param-template | sgs-service | sgtpc-service | subscriber-map | tai-mgmt-db }

no

Disassociates a previously associated service with this MME service.

egtp-service *egtp_svc_name*

Associates an eGTP service with MME service.
egtp_svc_name specifies the name for a pre-configured eGTP service to associate with the MME service. For more information on the eGTP service, refer to the **egtp-service** command in the *Context Configuration Mode Commands* chapter.

egtp-sv-service *egtp_sv_svc_name*

Associates an eGTP Sv service with this MME service.
egtp_sv_svc_name specifies the name for a pre-configured eGTP Sv service to associate with the MME service. For more information on the eGTP Sv service, refer to the **egtp-service** command in the *Context Configuration Mode Commands* chapter.

hss-peer-service *hss_svc_name*

Associates an HSS peer service with this MME service.
hss_svc_name specifies the name for a pre-configured HSS peer service to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information about the HSS peer service, refer to the **hss-peer-service** command in the *Context Configuration Mode Commands* chapter and the *HSS Peer Service Configuration Mode Commands* chapter.

lte-emergency-profile *profile_name*

Associates an LTE emergency profile with this MME service.
profile_name specifies the name for a pre-configured LTE emergency profile to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information about the LTE emergency

profile, refer to the **lte-emergency-profile** command in the *LTE Policy Configuration Mode Commands* chapter and the *LTE Emergency Profile Configuration Mode Commands* chapter.

---

network-global-mme-id-mgmt-db

Associates the configured global MME ID management database with the MME service. The global MME ID management database is configured through the LTE Policy Configuration Mode using the **network-global-mme-id-mgmt-db** command.

---

sctp-param-template *template_name*

Associates a Stream Control Transmission Protocol (SCTP) parameter template with the MME service.
template_name specifies the name for a pre-configured SCTP parameter template to associate with this MME service as an alphanumeric string of 1 through 63 characters. For more information on the SCTP parameter template, refer to the **sctp-param-template** command in the *Global Configuration Mode Commands* chapter and the *SCTP Parameter Template Configuration Mode Commands* chapter.

---

sgs-service *sgs_svc_name*

Associates an SGs service with this MME service.
sgs_svc_name specifies the name for a pre-configured SGs service to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information on the SGs service, refer to the **sgs-service** command in the *Context Configuration Mode Commands* chapter andthe *MME SGs Service Configuration Mode Commands* chapter.

---

sgtpc-service *sgtpc_svc_name*

Associates an SGTPC service with this MME service.
sgtpc_svc_name specifies the name for a pre-configured SGTPC service to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information on the SGTPC service, refer to the **sgtp-service** command in the *Context Configuration Mode Commands* chapter and/or the *SGTP Service Configuration Mode Commands* chapter.

---

context *ctx_name*

Identifies a specific context name where the named service is configured. If this keyword is omitted, the named service must exist in the same context as the MME service.
ctx_name is name of the configured context of the named service expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

---

subscriber-map *map_name*

Associates this MME service with a pre-configured subscriber map.
map_name specifies the name of a pre-configured subscriber map to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information on subscriber maps, refer to the **subscriber-map** command in the *LTE Policy Configuration Mode Commands* chapter andthe *LTE Subscriber Map Configuration Mode Commands* chapter.

---

tai-mgmt-db *database_name*

Associates this MME service with a pre-configured TAI Management Database.
database_name specifies the name of a pre-configured TAI Management Database to associate with the MME service as alphanumeric string of 1 through 64 characters. For more information on subscriber maps, refer to the **tai-mgmt-db** command in the *LTE Policy Configuration Mode Commands* chapter and the *LTE TAI Management Database Configuration Mode Commands* chapter.

Usage

Use this command to associate a pre-configured service or policy with an MME service.
The eGTP service provides eGTP-C protocol interface support between EPS nodes. For more information on the eGTP service and the supported interface type, refer to the *eGTP Service Configuration Mode Commands* chapter.

Important: Only one eGTP service can be associated with a service. The eGTP service should be configured prior to issuing this command.

The HSS peer service provides S6a and S13 interface support via the Diameter protocol between the MME and an HSS (S6a) or EIR (S13). For more information on HSS peer service and other parameters, refer to the *HSS Peer Service Configuration Mode Commands* chapter.

Important: Only one HSS peer service can be associated to a service in this release. The HSS peer service should be configured prior to issuing this command.

Caution: This is a critical configuration. The MME service cannot be started without this configuration. Any change to this configuration would lead to restarting the MME service. Removing or disabling this configuration will stop the MME service.

Example

The following command associates a pre-configured eGTP service called *egtp1* in the *dst_ctx* context to an MME service:

```
associate egtp-service egtp1 context dst_ctx
```

The following command associates a pre-configured HSS peer service called *hss1* in the same context as MME service to an MME service:

```
associate hss-peer-service hss1
```

bind s1-mme

Binds the MME service to a logical IP interface serving as the S1-MME interface.

Product

MME

Privilege

Administrator

Syntax

bind s1-mme { ipv4-address *address* **[ipv4-address** *secondary_address* **] | ipv6-address** *address* **[ipv6-address** *secondary_address* **] } [crypto-template** *name* **] [max-subscribers** *number* **]**

no bind s1-mme

no

Removes a previously configured IP address used for binding the SCTP (local bind address) to communicate with the eNodeBs using an S1-MME interface.

{ ipv4-address *address* **[ipv4-address** *secondary_address* **] | ipv6-address** *address* **[ipv6-address** *secondary_address* **] }**

Specifies the IP address for the interface configured as an S1-MME interface in IPv4 dotted-decimal or IPv6 colon-separated notation. Optionally configure a secondary IP address for either address type.

crypto-template *name*

Specifies an existing crypto template name used when implementing IP Security (IPSec) on the S1-MME interface. *name* is an alphanumeric string of 1 through 104 characters.

max-subscribers *number*

Specifies the maximum number of subscribers that can access this service on this interface as an integer from 0 through 4000000.

Usage

Use this command to associate the MME service with a specific logical IP address that will be used for binding the SCTP socket that communicates with the eNodeB using S1AP. Only one IP address can be configured with this command for one MME service.
The MME passes the IP address during setting up the SCTP association with the eNodeB.

Caution: This is a critical configuration. The MME service can not be started without this configuration. Any change to this configuration would lead to restarting the MME service and removing or disabling this configuration will stop the MME service.

Important: Up to two IPv4 or IPv6 addresses can be configured to support SCTP multi-homing.

Example

The following command would bind the logical IP interface with the address of *192.168.3.1* to the MME service to interact with eNodeB:

```
bind s1-mme ipv4-address 192.168.3.1
```

The following command disables a binding that was previously configured:

```
no bind s1-mme ipv4address
```

csg-change-notification

This command enables or disables the Closed Subscriber Group (CSG) Information reporting (notification) mechanism on the MME. When enabled, the MME includes the CSG Information Reporting Action IE with the appropriate Action field for subscribers.

Product

MME

Privilege

Administrator

Syntax

```
[ default | no ] csg-change-notification
```

default

Returns the command to its default value of disabled.

no

Disables the feature.

dns

Associates or disassociates the Domain Name System (DNS) client service configured for DNS query in a context to select P-GW and S-GW in an MME service.

Product

MME

Privilege

Administrator

Syntax

dns { peer-mme | peer-sgsn | pgw | sgw } [context *ctx_name* **]**

no dns { peer-mme | pgw | sgw }

no

Disassociates a previously associated context having DNS client service configured for DNS query to select peer MME, P-GW or S-GW with this MME service.

peer-mme

Associates the named context with a DNS client service for DNS query for selecting a peer MME and associating it with this MME service for inter-MME handovers.

peer-sgsn

Associates the named context with a DNS client service for DNS query for selecting a peer SGSN and associating it with this MME service for inter-RAT handovers.

pgw

Associates the named context with a DNS client service for DNS query for selecting a P-GW and associating it with this MME service.

sgw

Associates the named context with a DNS client service for DNS query for selecting an S-GW and associating it with this MME service.

context *ctx_name*

Optionally associates the specific context name where DNS client service is configured to select a peer MME, a P-GW and/or an S-GW for this MME service. If this keyword is omitted DNS client service must be configured in the same context as this MME service.
ctx_name is name of the configured context of the DNS client service expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage

Use this command to associate a pre-configured context where a DNS client service is configured with an MME service.

The DNS Client service configured in a context provides the DNS query support to locate peer MMEs, peer-SGSNs, P-GWs, or S-GWs from an MME service. For more information on DNS Client service and support, refer to the *DNS Client Service Configuration Mode Commands* chapter.
A maximum of one DNS client service for a peer MME, one DNS client service for a peer SGSN, one DNS client service for a P-GW, and one DNS client service for S-GW can be associated with an MME service.

Example

The following command associates a pre-configured context *dns_ctx1* where a DNS client service is configured for DNS query to P-GW from an MME service:

```
dns pgw context dns_ctx1
```

The following command associates a pre-configured context *dns_ctx2* where a DNS client service is configured for DNS query to S-GW from an MME service:

```
dns sgw context dns_ctx2
```

emm

Defines the Evolved Mobility Management timer parameters, such as timeout durations for timers and retransmission counts, for Non-Access Stratum (NAS) message retransmission in MME service.

Product

MME

Privilege

Administrator

Syntax

emm { implicit-detach-timeout *detach_dur* **| mobile-reachable-timeout** *mob_reach_dur* **| t3412-timeout** *t3412_dur* **| t3413-timeout** *t3413_dur* **| t3422-timeout** *t3422_dur* **| t3423-timeout** *t3423_dur* **| t3450-timeout** *t3450_dur* **| t3460-timeout** *t3460_dur* **| t3470-timeout** *t3470_dur* **}**

default emm { mobile-reachable-timeout | t3412-timeout | t3413-timeout | t3422-timeout | t3423-timeout | t3450-timeout | t3460-timeout | t3470-timeout }

no emm implicit-detach-timeout

default

Resets the specified timer timeout to the system default value.

no

Removes the specified EMM timeout definition from the configuration.

implicit-detach-timeout *detach_dur*

Sets the timer timeout duration (in seconds) after which subscriber will implicitly detached from the network if there is no activity. Generally this timer value is 240 seconds (4 minutes) more than the timeout value of the T3423 timer.
This timer starts when mobile reachable timer expires while the network is in EMM-IDLE mode and ISR is activated and stops when a NAS signalling connection established.
detach_dur is an integer from 1 through 12000. Default: 3480

mobile-reachable-timeout *mob_reach_dur*

Sets the timeout timer duration (in seconds) after which reachability procedure will be discarded and reattempt starts.
mob_reach_dur is an integer from 1 through 12000. Default: 3480

t3412-timeout *t3412_dur*

Sets the timeout duration (in seconds) for the T3412 timer. This timer is used for periodic tracking area update (P-TAU). When this timer expires, the periodic tracking area updating procedure starts and the timer is set to its initial value for the next start.
This timer starts when the UE goes from EMM-CONNECTED to EMM-IDLE mode and stops when the UE enters EMM-CONNECTED mode.
t3412_dur is an integer from 1 through 11160. Default: 3240

t3413-timeout *t3413_dur*

Sets the timeout duration (in seconds) for the T3413 timer. The timer starts when MME initiates the EPS paging procedure to the EMM entity in the network and requests the lower layer to start paging. This timer stops for the paging procedure when a response received from the UE.
t3413_dur is an integer from 1 through 20. Default: 6

t3422-timeout *t3422_dur*

Sets the timeout duration (in seconds) for the T3422 timer. This timer starts when MME initiates the detach procedure by sending a DETACH REQUEST message to the UE and stops upon receipt of the DETACH ACCEPT message.
t3422_dur is tan integer from 1 through 20. Default: 6

t3423-timeout *t3423_dur*

Sets the timeout duration (in seconds) for the T3423 timer. This timer starts when UE enters the EMM-DEREGISTERED state or when entering EMM-CONNECTED mode. It stops while the UE is in EMM-REGISTERED.NO-CELL-AVAILABLE state and Idle mode Signalling Reduction (ISR) is activated.
t3423_dur is an integer from 1 through 11160. Default: 3240

t3450-timeout *t3450_dur*

Sets the timeout duration (in seconds) for the T3450 timer. This timer starts when MME initiates the Globally Unique Temporary Identifier (GUTI) reallocation procedure by sending a GUTI REALLOCATION COMMAND message to the UE and stops upon receipt of the GUTI REALLOCATION COMPLETE message.
This timer is also used for the Tracking Area update procedure.
t3450_dur is an integer from 1 through 20. Default: 6

t3460-timeout *t3460_dur*

Sets the timeout duration (in seconds) for the T3460 timer. This timer starts when the network initiates the authentication procedure by sending an AUTHENTICATION REQUEST message to the UE and stops upon receipt of the AUTHENTICATION RESPONSE message.
t3460_dur is an integer from 1 through 20. Default: 6

t3470-timeout *t3470_dur*

Sets the timeout duration (in seconds) for the T3470 timer. The MME starts this timer when the network initiates the identification procedure by sending an IDENTITY REQUEST message to the UE and stops upon receipt of the IDENTITY RESPONSE message.
t3470_dur is an integer from 1 through 20. Default: 6

Usage

Use this command to set EMM timers.
The following tables describe the triggers and states for timers:

Table 25. EPS Mobility Management Timers – UE Side

Timer	State	Cause of Start	Normal Stop	On Expiry

Timer	State	Cause of Start	Normal Stop	On Expiry
T3402	• EMM-DEREGISTERED • EMM-REGISTERED	• At attach failure and the attempt counter is equal to 5. • At tracking area updating failure and the attempt counter is equal to 5.	• ATTACH REQUEST sent • TRACKING AREA UPDATE REQUEST sent	Initiation of the attach procedure or TAU procedure
T3410	EMM-REGISTERED-INITIATED	ATTACH REQUEST sent	• ATTACH ACCEPT received • ATTACH REJECT received	Start T3411 or T3402 as described in subclause 5.5.1.2.6
T3411	• EMM-DEREGISTERED. ATTEMPTING-TO-ATTACH • EMM-REGISTERED. ATTEMPTING-TO-UPDATE	• At attach failure due to lower layer failure, T3410 timeout or attach rejected with other EMM cause values than those treated in subclause 5.5.1.2.5. • At tracking area updating failure due to lower layer failure, T3430 timeout or TAU rejected with other EMM cause values than those treated in subclause 5.5.3.2.5.	• ATTACH REQUEST sent • TRACKING AREA UPDATE REQUEST sent	Retransmission of the ATTACH REQUEST or TRACKING AREA UPDATE REQUEST
T3412	EMM-REGISTERED	In EMM-REGISTERED, when EMM-CONNECTED mode is left.	• When entering state EMM-DEREGISTERED or • When entering EMM-CONNECTED mode.	Initiation of the periodic TAU procedure

Timer	State	Cause of Start	Normal Stop	On Expiry
T3416	• EMM-REGISTERED-INITIATED • EMM-REGISTERED • EMM-DEREGISTERED-INITIATED • EMM-TRACKING-AREA-UPDATING-INITIATED • EMM-SERVICE-REQUEST-INITIATED	RAND and RES stored as a result of a UMTS authentication challenge	• SECURITY MODE COMMAND received • SERVICE REJECT received • TRACKING AREA UPDATE ACCEPT received • AUTHENTICATION REJECT received • AUTHENTICATION FAILURE sent • EMM-DEREGISTERED or EMM-NULL entered	Delete the stored RAND and RES
T3417	EMM-SERVICE-REQUEST-INITIATED	• SERVICE REQUEST sent • EXTENDED SERVICE REQUEST sent in case f and g in subclause 5.6.1.1	• Bearers have been set up • SERVICE REJECT received	Abort the procedure
T3417ext	EMM-SERVICE-REQUEST-INITIATED	• EXTENDED SERVICE REQUEST sent in case d in subclause 5.6.1.1 • EXTENDED SERVICE REQUEST sent in case e in subclause 5.6.1.1 and the CSFB response was set to “CS fallback accepted by the UE”.	• Inter-system change from S1 mode to A/Gb mode or Iu mode is completed • Inter-system change from S1 mode to A/Gb mode or Iu mode is failed • SERVICE REJECT received	Abort the procedure

Timer	State	Cause of Start	Normal Stop	On Expiry
T3418	• EMM-REGISTERED-INITIATED • EMM-REGISTERED • EMM-TRACKING-AREA-UPDATING-INITIATED • EMM-DEREGISTERED-INITIATED • EMM-SERVICE-REQUEST-INITIATED	AUTHENTICATION FAILURE (EMM cause = #20 “MAC failure” or #26 “Non-EPS authentication unacceptable”) sent	AUTHENTICATION REQUEST received	On first expiry, the UE should consider the network as false
T3420	• EMM-REGISTERED-INITIATED • EMM-REGISTERED • EMM-DEREGISTERED-INITIATED • EMM-TRACKING-AREA-UPDATING-INITIATED • EMM-SERVICE-REQUEST-INITIATED	AUTHENTICATION FAILURE (cause = #21 “synch failure”) sent	AUTHENTICATION REQUEST received	On first expiry, the UE should consider the network as false
T3421	EMM-DEREGISTERED-INITIATED	DETACH REQUEST sent	DETACH ACCEPT received	Retransmission of DETACH REQUEST

Timer	State	Cause of Start	Normal Stop	On Expiry
T3423	EMM-REGISTERED	T3412 expires while the UE is in EMM-REGISTERED.NO-CELL-AVAILABLE and ISR is activated.	• When entering state EMM-DEREGISTERED or • When entering EMM-CONNECTED mode.	Set TIN to "P-TMSI"
T3430	EMM-TRACKING-AREA-UPDATING-INITIATED	TRACKING AREA UPDATE REQUEST sent	• TRACKING AREA UPDATE ACCEPT received • TRACKING AREA UPDATE REJECT received	Start T3411 or T3402 as described in subclause 5.5.3.2.6
T3440	• EMM-REGISTERED-INITIATED • EMM-TRACKING-AREA-UPDATING-INITIATED • EMM-DEREGISTERED-INITIATED • EMM-SERVICE-REQUEST-INITIATED • EMM-REGISTERED	• ATTACH REJECT, DETACH REQUEST, TRACKING AREA UPDATE REJECT with any of the EMM cause values #11, #12, #13, #14 or #15 • SERVICE REJECT received with any of the EMM cause values #11, #12, #13 or #15 • TRACKING AREA UPDATE ACCEPT received after the UE sent TRACKING AREA UPDATE REQUEST in EMM-IDLE mode with no "active" flag	• Signalling connection released • Bearers have been set up	Release the signalling connection and proceed as described in subclause 5.3.1.2
T3442	EMM-REGISTERED	SERVICE REJECT received with EMM cause #39	TRACKING AREA UPDATE REQUEST sent	None
NOTE 1: The default value of this timer is used if the network does not indicate another value in an EMM signalling procedure.				
NOTE 2: The value of this timer is provided by the network operator during the attach and tracking area updating procedures.				
NOTE 3: The value of this timer may be provided by the network in the ATTACH ACCEPT message and TRACKING AREA UPDATE ACCEPT message. The default value of this timer is identical to the value of T3412.				

Timer	State	Cause of Start	Normal Stop	On Expiry
NOTE 4: The value of this timer is provided by the network operator when a service request for CS fallback is rejected by the network with EMM cause #39 “CS domain temporarily not available”.				

Table 26. EPS Mobility Management Timers – Network Side

Timer	State	Cause of Start	Normal Stop	On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)
T3413	EMM-REGISTERED	Paging procedure initiated	Paging procedure completed	Network dependent
T3422	EMM-DEREGISTERED-INITIATED	DETACH REQUEST sent	DETACH ACCEPT received	Retransmission of DETACH REQUEST
T3450	EMM-COMMON-PROC-INIT	• ATTACH ACCEPT sent • TRACKING AREA UPDATE ACCEPT sent with GUTI • GUTI REALLOCATION COMMAND sent	• ATTACH COMPLETE received • TRACKING AREA UPDATE COMPLETE received • GUTI REALLOCATION COMPLETE received	Retransmission of the same message type, i.e. ATTACH ACCEPT, TRACKING AREA UPDATE ACCEPT or GUTI REALLOCATION COMMAND
T3460	EMM-COMMON-PROC-INIT	• AUTHENTICATION REQUEST sent • SECURITY MODE COMMAND sent	• AUTHENTICATION RESPONSE received • AUTHENTICATION FAILURE received • SECURITY MODE COMPLETE received • SECURITY MODE REJECT received	Retransmission of the same message type, i.e. AUTHENTICATION REQUEST or SECURITY MODE COMMAND
T3470	EMM-COMMON-PROC-INIT	IDENTITY REQUEST sent	IDENTITY RESPONSE received	Retransmission of IDENTITY REQUEST
Mobile reachable timer	All except EMM-DEREGISTERED	Entering EMM-IDLE mode	NAS signalling connection established	Network dependent, but typically paging is halted on 1st expiry
Implicit detach timer	All except EMM-DEREGISTERED	The mobile reachable timer expires while the network is in EMM-IDLE mode and ISR is activated	NAS signalling connection established	Implicitly detach the UE on 1st expiry

Timer	State	Cause of Start	Normal Stop	On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)
NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.				
NOTE 2: The value of this timer is network dependent.				

Table 27. EPS Session Management Timers – UE Side

Timer	State	Cause of Start	Normal Stop	On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)
T3480	PROCEDURE TRANSACTION PENDING	BEARER RESOURCE ALLOCATION REQUEST sent	ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST received or MODIFY EPS BEARER CONTEXT REQUEST received or BEARER RESOURCE ALLOCATION REJECT received	Retransmission of BEARER RESOURCE ALLOCATION REQUEST
T3481	PROCEDURE TRANSACTION PENDING	BEARER RESOURCE MODIFICATION REQUEST sent	ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST received or MODIFY EPS BEARER CONTEXT REQUEST received or DEACTIVATE EPS BEARER CONTEXT REQUEST received or BEARER RESOURCE MODIFICATION REJECT received	Retransmission of BEARER RESOURCE MODIFICATION REQUEST
T3482	PROCEDURE TRANSACTION PENDING	An additional PDN connection is requested by the UE which is not combined in attach procedure	ACTIVE DEFAULT EPS BEARER CONTEXT REQUEST received or PDN CONNECTIVITY REJECT received	Retransmission of PDN CONNECTIVITY REQUEST
T3492	PROCEDURE TRANSACTION PENDING	PDN DISCONNECT REQUEST sent	DEACTIVATE EPS BEARER CONTEXT REQUEST received or PDN DISCONNECT REJECT received	Retransmission of PDN DISCONNECT REQUEST
NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.				

This command can be repeated to set each timer as needed.
The retransmission of all type of NAS messages can be configured through **`nas-max-retransmissions`** command.

Example

The following command sets the timeout value for EPS paging procedure timer T3413 for *10* seconds.

```
emm t3413-timeout 10
```

enb-cache-timeout

Configures the amount of time that eNodeB information is stored in cache after the eNodeB terminates the connection.

Product

MME

Privilege

Administrator

Syntax

enb-cache-timeout *min*

default enb-cache-timeout

default

Returns the command to its default value of 10.

min

Specifies the amount of time (in minutes) that the MME stores eNodeB information after the eNodeB terminates the connection. *min* is an integer value from 1 through 1440. Default: 10
In releases prior to 12.2, *min* is an integer value from 1 through 60.

Usage

Use this command to set the amount of time the MME stores eNodeB information in cache after the eNodeB terminates the connection.

Example

The following command sets the amount of time the MME stores eNodeB information to *15* minutes:

```
enb-cache-timeout 15
```

encryption-algorithm-lte

Configures the precedence for LTE encryption algorithms to use for security procedures through this MME service.

Product

MME

Privilege

Administrator

Syntax

```
encryption-algorithm-lte priority1 { 128-eea0 | 128-eea1 | 128-eea2 } [ priority2 { 128-eea0 | 128-eea1 | 128-eea2 } ] [ priority3 { 128-eea0 | 128-eea1 | 128-eea2 } ]

default encryption-algorithm-lte
```

default

Sets the default LTE encryption algorithm for security procedures with configured priority *value*. Lowest value has highest preference. Default configuration of LTE encryption algorithm is:

- priority1 with 128-eea0 encryption algorithm
- priority2 with 128-eea1 encryption algorithm
- priority3 with 128-eea2 encryption algorithm

priority1

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 1.

priority2

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 2.

priority3

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 3.

128-eea0

Sets the Null ciphering algorithm (128-EEA0) for LTE encryption as the encryption algorithm for security procedures. Default: Enabled

128-eea1

This keyword sets the SNOW 3G synchronous stream ciphering algorithm (128-EEA1) for LTE encryption as the encryption algorithm for security procedures. SNOW 3G is a stream cipher that forms the base of the 3GPP confidentiality algorithm UEA2 and the 3GPP integrity algorithm UIA2. Default: priority2

128-eea2

Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EEA2) for LTE encryption as the encryption algorithm for security procedures. Default: priority3

Usage

Use this command to set the LTE encryption algorithms for security procedures to use with this MME service.

Caution: When this command is executed, all the existing priority-to-algorithm mappings will be removed and the newly configured ones will be applicable for security procedures.

Caution: Configuration of the same algorithm to multiple priorities is prohibited.

Example

The following command sets the 128-EEA1 as the LTE encryption algorithm with priority 2 for security procedures with an MME service:

```
encryption-algorithm-lte priority2 128-eea1
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

esm

Defines the Evolved Session Management timer parameters like timeout durations for timers and retransmission counts for the retransmission of Non-Access Stratum (NAS) messages in MME service.

Product

MME

Privilege

Administrator

Syntax

esm { t3485-timeout *t3485_dur* **| t3486-timeout** *t3486_dur* **| t3489-timeout** *t3489_dur* **| t3495-timeout** *t3495_dur* **}**

default esm { t3485-timeout | t3486-timeout | t3489-timeout | t3495-timeout }

default

Resets the specified Evolved Session Management timer timeout to the system default value.

t3485-timeout *t3485_dur*

Sets the timeout duration (in seconds) for the T3485 timer. This timer is used by the default EPS bearer context activation procedure.
This timer starts when the MME sends an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message to UE and stops when receives ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT or ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message from UE.
t3485_dur is an integer from 1 through 60. Default: 8

t3486-timeout *t3486_dur*

Sets the timeout duration (in seconds) for theT3486 timer. This timer is used by the default EPS bearer context modification procedure.
This timer starts when the MME sends a MODIFY EPS BEARER CONTEXT REQUEST message to the UE and stops when it receives a MODIFY EPS BEARER CONTEXT ACCEPT received or a MODIFY EPS BEARER CONTEXT REJECT message from UE.
t3485_dur is an integer from 1 through 60. Default: 8

t3489-timeout *t3489_dur*

Sets the timeout duration (in seconds) for the T3489 timer. This timer is used for the default EPS bearer context deactivation procedure.
This timer starts when the MME sends an ESM INFORMATION REQUEST message to the UE and stops when receives a ESM INFORMATION RESPONSE message from the UE.
t3495_dur is an integer from 1 through 60. Default: 4

t3495-timeout *t3495_dur*

Sets the timeout duration (in seconds) for the T3495 timer. This timer is used for default EPS bearer context deactivation procedure.

This timer starts when the MME sends a DEACTIVATE EPS BEARER CONTEXT REQUEST message to UE and stops when receives DEACTIVATE EPS BEARER CONTEXT ACCEPT or DEACTIVATE EPS BEARER CONTEXT REJECT message from UE.
t3495_dur is tan integer from 1 through 60. Default: 8

Usage

Use this command to set Evolved Session Management timers.
the following tables describe the triggers and states for timers:

Table 28. EPS Session Management Timers – Network Side

Timer	State	Cause of Start	Normal Stop	On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)
T3485	BEARER CONTEXT ACTIVE PENDING	• ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST sent • ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST sent	• ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT received or • ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT received or • ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT received or • ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT received	Retransmission of the same message
T3486	BEARER CONTEXT MODIFY PENDING	MODIFY EPS BEARER CONTEXT REQUEST sent	• MODIFY EPS BEARER CONTEXT ACCEPT received or • MODIFY EPS BEARER CONTEXT REJECT received	Retransmission of MODIFY EPS BEARER CONTEXT REQUEST

Timer	State	Cause of Start	Normal Stop	On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)
T3489	PROCEDURETRANSACTION PENDING	ESM INFORMATION REQUEST sent	ESM INFORMATION RESPONSE received	Retransmission of ESM INFORMATION REQUEST on 1st and 2nd expiry only
T3495	BEARER CONTEXT INACTIVE PENDING	DEACTIVATE EPS BEARER CONTEXT REQUEST sent	DEACTIVATE EPS BEARER CONTEXT ACCEPT received	Retransmission of DEACTIVATE EPS BEARER CONTEXT REQUEST
NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.				

This command can be repeated to set each timer as needed.
The retransmission of all type of NAS messages can be configured through **nas-max-retransmissions** command.

Example

The following command sets the timeout value for the default EPS bearer context activation procedure timer (T3485) for 10 seconds.

```
esm t3485-timeout 10
```

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

gtpv2

Configures GTPv2 piggybacking support from the MME to the P-GW. A piggybacking flag is sent by the MME to a P-GW in the S11 “Create Session Request” message and determines whether dedicated bearer creation (Create Bearer Request) is piggybacked onto the “Create Session Response” message or not.

Product

MME

Privilege

Administrator

Syntax

```
[ default | no ] gtpv2 piggybacking
```

default

Returns the command to its default setting of enabled.

no

Disables the feature.

piggybacking

Specifies that piggybacking is to be performed by the P-GW.

Usage

Use this command to enable the sending of a piggybacking flag to the P-GW over the S11 interface requesting that the Create Bearer Request message is piggybacked on the Create Session Response message (sent from the P-GW to the MME.

Example

The following command disables this feature:

```
no gtpv2 piggybacking
```

heuristic-paging

Enables or disables the heuristic or optimized paging feature for the service.

Product

MME

Privilege

Administrator

Syntax

```
[ default | no ] heuristic-paging
```

default

Returns the command to its default setting of disabled.

no

Disables the feature.

Usage

Use this command to enable or disable the heuristic paging feature for the service. Also known as idle-mode paging, enabling this feature prompts the MME service to keep track of the eNodeBs to which the access terminal (AT) most commonly attaches, thus reducing the signalling otherwise associated with continuous paging.

Important: Optimized Paging is a licensed feature and will not appear as a command option unless the proper licensed is installed.

integrity-algorithm-lte

Configures the precedence of LTE integrity algorithms to use for security procedures through this MME service. By default the integrity algorithm is enabled on MME service and cannot be disabled.

Product

MME

Privilege

Administrator

Syntax

```
integrity-algorithm-lte priority1 { 128-eia1 | 128-eia2 } [ priority2 { 128-eia1 | 128-eia2 } ]

default integrity-algorithm-lte
```

default

Removes the preconfigured integrity algorithm and sets the default LTE integrity algorithm for security procedures. Default configuration of LTE integrity algorithm is:

- priority1 with 128-eia1 integrity algorithm
- priority2 with 128-eia2 integrity algorithm

priority1

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 1. This is the mandatory and default priority keyword.

priority2

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 2.

128-eia1

This keyword sets the SNOW 3G synchronous stream ciphering algorithm (128-EIA1) for LTE integrity as the integrity algorithm for security procedures. SNOW 3G is a stream cipher that forms the base of the 3GPP confidentiality algorithm UEA2 and the 3GPP integrity algorithm UIA2. Default: priority1

128-eia2

Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EIA2) for LTE integrity as the integrity algorithm for security procedures. Default: Enabled

Usage

Use this command to set the LTE integrity algorithms for security procedures to use with this MME service.

WARNING: Integrity algorithm is a mandatory aspect and can not be disabled in MME service.

Caution: When this command is executed, all the existing priority to algorithm mappings will be removed and the newly configured ones will be applicable for security procedures.

Caution: Configuration of same algorithm to multiple priorities is prohibited.

Example

The following command sets the AES ciphering algorithms (128-EIA2) as the LTE integrity algorithm with priority as *1* for security procedures with an MME service:

```
integrity-algorithm-lte priority1 128-eia2
```

location-reporting

Enables or disables the UE location reporting function on the MME service.

Product

MME

Privilege

Administrator

Syntax

```
[ no | default ] location-reporting
```

default

Disables the location reporting feature on MME service.

no

Disables the location reporting feature on MME service.

Usage

Use this command to enable or disable the UE location reporting feature on the MME service. When enabled the MME forwards a location report request for a specific UE from the P-GW to the eNodeB.

Important: Location reporting, also known as User Location Information (ULI) Reporting, is a licensed feature and requires the purchase of the ULI Reporting feature license.

Example

The following command sets the MME service to allow for location reporting for UEs:

```
location-reporting
```

max-bearers per-subscriber

Specifies the maximum number of EPS bearers that a subscriber may simultaneously use to access this MME service.

Product

MME

Privilege

Administrator

Syntax

max-bearers per-subscriber *max_bearer*

default max-bearers per-subscriber

default

Configures the maximum EPS bearers for a subscriber to use simultaneously to the default value of 11.

max_bearer

Specifies the maximum number of EPS bearers for a subscriber may simultaneously use to access this MME service.
max_bearer is an integer from 1 through 11. Default: 11

Usage

Use this command to set the maximum number of EPS bearers that a subscriber may simultaneously use to access this MME service.

Example

The following command specifies that a maximum of *6* simultaneous EPS bearers can be facilitated for a subscriber at any given time:

```
max-bearers per-subscriber 6
```

max-paging-attempts

This command configures the maximum number of paging attempt retransmissions allowed for network requested service creation to a subscriber after the first attempt failed.

Product

MME

Privilege

Administrator

Syntax

max-paging-attempts *max_paging_retry*

default max-paging-attempts

default

Configures the maximum number of paging request retransmissions to the default value of 3.

max_paging_retry

Specifies the maximum number of paging attempt retransmissions allowed for network requested service creation to a subscriber after the first attempt failed.
max_paging_retry is an integer from 1 through 10. Default: 3

Usage

Use this command to set the maximum number of paging attempt retransmissions allowed for network requested service creation to a subscriber after the first attempt failed.

Example

The following command specifies that a maximum of *6* paging attempt retransmissions allowed for network requested service creation to a subscriber:

```
max-paging- 6
```

max-pdns per-subscriber

Specifies the maximum number of Packet Data Networks (PDNs) that a subscriber may simultaneously access through this MME service.

Product

MME

Privilege

Administrator

Syntax

max-pdns per-subscriber *max_pdn*

default max-pdns per-subscriber

default

Configures the maximum PDNs that a subscriber can simultaneously access through this MME service to the default value of 3.

max_pdn

Specifies the maximum number of PDNs that a subscriber may simultaneously access through this MME service.
max_pdn is an integer from 1 through 11. Default: 3

Usage

Use this command to set the maximum number of PDNs that a subscriber may simultaneously access through this MME service.

Example

The following command specifies that a maximum of *2* simultaneous PDNs can be accessed by a subscriber at any given time through this MME service:

```
max-pdns per-subscriber 2
```

mme-id

Configures the MME identifier within an MME service. The MME identifier is constructed form the MME group ID and MME Code.

Product

MME

Privilege

Administrator

Syntax

mme-id group-id *grp_id* **mme-code** *mme_code*

no mme-id

no

Removes the configured MME identifier for this MME service.

Caution: Removing the MME identifier is a disruptive operation; the MME service is removed from the system.

group-id *grp_id*

Specifies the group identifier for the group of which this MME belongs as an integer from 0 through 65535.

mme-code *mme_code*

Specifies the unique code for this MME service as an integer from 0 through 255.

Usage

Use this command to set the MME identifier for this MME service. This MME identifier will be the identity of this MME in network.

Caution: Changing or removing the MME identifier is a disruptive operation; the MME service will be re-started or removed from service.

Example

The following command configures the MME identifier with group id as *41025* and MME code as *101* for this MME service:

```
mme-id group-id 41025 mme-code 101
```

mmemgr-recovery

Configures the recovery action for the MME manager.

Product

MME

Privilege

Administrator

Syntax

```
mmemgr-recovery { no-reset | reset-s1-peers }

default mmemgr-recovery
```

default

Resets the command to its default value.

no-reset

Specifies that the recovery action is to NOT reset S1 peers.

reset-s1-peers

Specifies that the recovery action is TO reset S1 peers.

Usage

Use this command to set a recovery action for the MME Manager.

Example

The following command configures the MME Manager recovery action to reset all S1 peers:

```
mmemgr-recovery reset-s1-peers
```

msc

Specifies the IP address of the enhanced Mobile Switching Center (eMSC) server for the MME service. This parameter is used for communicating with the eMSC server over the Sv interface in support of the Single Radio Voice Call Continuity (SRVCC) feature.

Product

MME

Privilege

Administrator

Syntax

msc *ip_address*

no msc

no

Removes the eMSC IP address configuration from the MME service.

ip_address

Specifies the IP address of the peer eMSC server in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to specify the IP address of the peer eMSC server used during SRVCC handovers.

Example

The following command specifies an IPv4 address for the peer eMSC server as *10.2.3.4*:

```
msc 10.2.3.4
```

nas-max-retransmission

Sets the retransmission counter for all type of Non-Access Stratum (NAS) messages in an MME service.

Product

MME

Privilege

Administrator

Syntax

nas-max-retransmissions *nas_retrans_count*

default nas-max-retransmissions

default

Resets the retransmission counter to the default value of 4.

nas_retrans_count

Sets the maximum number of retransmission of NAS messages permitted during any procedure after which the activation procedure will be discarded.
nas_retrans_count is an integer from 1 through 10. Default: 4

Usage

Use this command to set maximum number of retries allowed for any type of NAS messages.
NAS Messages sent by the MME which require a response from the UE for procedure completion are retransmitted. Retransmission happens based on timer expiry. The timers are configured through the **emm** and **esm** commands. NAS messages are retransmitted per configuration, and if no response is received from the UE, the pending transaction is abandoned. If the transaction is a DETACH or PDN DISCONNECT REQUEST, the transaction is completed without further UE signaling.
The timeout duration configured through the **emm** and **esm** commands will be applicable between two retries.

Example

The following command sets the maximum number of retries allowed as *4* for all type of NAS messages in an MME service.

```
default nas-max-retransmissions
```

network-sharing

Configures additional PLMN IDs for this MME service. Refer to the **plmn-id** command to create the base PLMN identifier for an MME service. Each PLMN ID consists of the Mobile Country Code (MCC) and Mobile Network Code (MNC). A maximum of four network sharing entries can be configured per MME service. These PLMN IDs will be communicated to the eNodeBs in the S1 SETUP response and MME CFG Update messages.

Product

MME

Privilege

Administrator

Syntax

network-sharing plmnid mcc *number* **mnc** *number* **mme-id group-id** *id* **mme-code** *code*

no network-sharing plmnid mcc *number* **mnc** *number*

no

Disables the network sharing mode on this MME service.

Caution: Removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

plmnid mcc *number* **mnc** *number*

Sets the mobile country code (MCC) and mobile network code (MNC) of the PLMN ID for this service.
mcc *number*: Specifies the MCC portion of the PLMN identifier as an integer from 100 through 999.
mnc *number*: Specifies the MNC portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

mme-id group-id *id*

Specifies the group identifier for the group to which this MME belongs as an integer from 0 through 65535.

mme-code *code*

Specifies the unique code for an MME service as an integer from 0 through 255.

Usage

Use this command to configure additional PLMN IDs for an MME service. In a given MME service, each PLMN ID (MCC and MNC) must be unique.

Caution: Changing or removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

Example

The following command configures the network sharing parameters to an MCC of *123*, an MNC of *12*, a MME-ID/Group ID of *100*, and a MME code of *50*:

```
network-sharing plmnid mcc 123 mnc 12 mme-id group-id 100 mme-code 50
```

nri

Configures the network resource identifier (NRI) length used for source SGSN discovery via NRI-FQDN (Fully Qualified Domain Name) based DNS resolution.

Product

MME

Privilege

Administrator

Syntax

[no] nri length *length* **plmn-id mcc** *mcc_value* **mnc** *mnc_value*

no

Removes a configured NRI length.

length *length*

Specifies the number of bits to be used in the P-TMSI (bits 23 to 18) to define the NRI as an integer from 1 through 8.

plmn-id mcc *mcc_value* **mnc** *mnc_value*

Specifies the PLMN-ID of the SGSN pool.
mcc *mcc_value*: Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.
mnc *mnc_value*: Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

Usage

Use this command to retrieve the NRI (identity of an SGSN) stored in bits 23 to 18 of the packet-temporary mobile subscriber identity (P-TMSI). Up to eight NRI length values can be configured.

Important: In the absence of this configuration, the MME treats the NRI as invalid. The MME will use a plain RAI-based FQDN (and not an NRI-based FQDN) for DNS queries made to resolve the source SGSN.

Example

The following command creates an NRI length of *5* and associates it with an SGSN pool with the PLMN-ID of *123*:

```
nri length 5 plmnid mcc 123 mnc 23
```

peer-mme

Configures parameters that, when matched by another MME, specifies that MME as a peer for inter-MME relocations.

Product

MME

Privilege

Administrator

Syntax

peer-mme { gummei mcc *number* **mnc** *number* **group-id** *id* **mme-code** *code* **address** *ipv4_address* **| tai-match priority** *value* **mcc** *number* **mnc** *number* **tac {** *area_code* **| any |** *start_area_code* **to** *end_area_code* **} address** *ipv4_address* **}**

no peer-mme { gummei mcc *number* **mnc** *number* **group-id** *id* **mme-code** *code* **| tai-match priority** *value*

---

no

Removes the configured peer Globally Unique MME Identifier (GUMMEI) or TAI match priority from this service.

---

gummei mcc *number* **mnc** *number* **group-id** *id* **mme-code** *code* **address** *ipv4_address*

Specifies that an MME with values matching those configured in this GUMMEI is to be considered a peer MME. This variable supports the lookup of an IP address for a peer MME based on the exact match of the supporting keyword below (which make up the GUMMEI).
mcc *number*: Sets the mobile country code (MCC) for peer match as an integer from 100 through 999.
mnc *number*: Sets the mobile network code (MNC) for this peer match as a 2- or 3-digit integer from 00 through 999.
group-id *id*: Specifies the group identifier for the group to which this MME belongs as an integer from 32768 through 65535.
mme-code *code*: Specifies the unique code for an MME service as an integer from 0 through 255.
address *ipv4_address*: Specifies the IP address of the peer MME in IPv4 dotted-decimal notation.

---

tai-match priority *value* **mcc** *number* **mnc** *number* **tac {** *area_code* **| any |** *start_area_code* **to** *end_area_code* **} address** *ipv4_address*

Specifies that an MME with values matching those configured in this Tracking Area Identifier (TAI) match, is to be considered a peer MME. This keyword provides a priority-ordered list of TAI descriptions where the Tracking Area Code (TAC) field may be either an exact value, a range of values, or a “wildcard” value. It also provides an IP address of the peer MME corresponding to the TAI description.
priority *value*:
mcc *number*: Sets the mobile country code (MCC) for peer match as an integer from 100 through 999.
mnc *number*: Sets the mobile network code (MNC) for this peer match as an integer from 00 through 999.
tac *area_code*: Sets a specific Tracking Area Code (TAC) for the peer MME match as an integer from 1 through 65535.
tac any: Specifies that any TAC value can be considered for a peer MME.
tac *start_area_code* **to** *end_area_code*: Specifies a range of TACs. MMEs within this range and matching the rest of the criteria in this command are to be considered peer MMEs. *start_area_code* and *end_area_code* are integers from 1 through 268435455.

address *ipv4_address*: Sets a specific IP address for this TAI peer MME match in IPv4 dotted-decimal notation.

Usage

Use this command to configure parameters that, when matched by another MME, specifies that MME as a peer for inter-MME relocations.
This command allows configuration for two relocation scenarios:

- **gummei**: an MME receives either an Attach or a TAU request with a Globally Unique Temporary Identity (GUTI) that originated from another MME.
- **tai-match**: an MME receives an S1 Handover Required message and must select a new MME based on the TAI.

Up to 32 peer-mme gummei or tai-match entries may be configured per MME service.

Example

The following command identifies a peer MME with GUMMEI parameters:

```
peer-mme gummei mcc 123 mnc 12 group-id 40000 mme-code 100 address
10.2.3.4
```

peer-sgsn

Statically configures peer SGSN environments to facilitate MME-SGSN relocations over S3 or Gn/Gp interfaces.

Product

MME

Privilege

Administrator

Syntax

peer-sgsn rai mcc *mcc_value* **mnc** *mnc_value* **[nri** *value* **] rac** *value* **lac** *value* **address** *ip_address* **capability [gn] [gp] [s16] [s3]**

no peer-sgsn rai mcc *mcc_value* **mnc** *mnc_value* **[nri** *value* **] rac** *value* **lac** *value*

peer-sgsn rnc-id mcc *mcc_value* **mnc** *mnc_value* **rnc** *value* **address** *ip_address* **capability [gn] [gp] [s16] [s3]**

no peer-sgsn rnc-id mcc *mcc_value* **mnc** *mnc_value* **rnc** *value*

rai

Configures Routing Area Identity (RAI) parameters used to facilitate a lookup for a specific peer SGSN.

rnc-id

Configures Radio Network Controller Identification (RNC-ID) parameters used to facilitate a lookup for a specific peer SGSN.

mcc *mcc_value*

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

mnc *mnc_value*

Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

nri *value*

Specifies the Network Resource Identifier (NRI) value used as an additional identity along with the RAC within the RAI parameters as an integer from 0 through 65535.

rac *value*

Specifies the Routing Area Code (RAC) used to facilitate a lookup for a specific peer SGSN as an integer from 0 through 255.

rnc *value*

Specifies the Radio Network Controller (RNC) identification number used to facilitate a lookup for a specific peer SGSN as an integer from 0 through 65535.

lac *value*

Specifies the Location Area Code (LAC) value used to facilitate a lookup for a specific peer SGSN as an integer from 0 through 65535.

address *ip_address*

Specifies an existing IP address of the peer SGSN in IPv4 dotted-decimal or IPv6 colon-separated notation.

capability [gn] [gp] [s16] [s3]

Configures the GTP interface capability of the peer SGSN.
gn: Specifies that the peer SGSN is capable of communication over the Gn interface.
gp: Specifies that the peer SGSN is capable of communication over the Gp interface.
s16: Specifies that the peer SGSN is capable of communication over the S16 interface.
s3: Specifies that the peer SGSN is capable of communication over the S3 interface.

Usage

Use this command to configure parameters that, when matched by an SGSN, specifies that SGSN as a peer for inter-RAT relocations.
This command allows configuration for two relocation scenarios:

- **rai**: the lookup of an IP address for a peer MME based on the exact match of the RAI (and optionally NRI).
- **rnc-id**: the lookup of an IP address for a peer SGSN based on the exact match of the RNC-ID.

Up to 32 peer-SGSN RAI and RNC-ID entries may be configured per MME service.

Example

The following command configures an SGSN lookup using RNC-ID parameters with Gn interface capability:

```
peer-sgsn rnc-id mcc 123 mnc 12 rnc 2000 address 10.2.3.4 capability gn
```

pgw-address

Configures the PDN Gateway (P-GW) address, specifies the protocol for S5 and S8 interfaces, and sets other parameters within the MME service. By default S5 and S8 use GTP protocol for this.

Product

MME

Privilege

Administrator

Syntax

pgw-address *address* **[s5-s8-protocol pmip] [weight** *value* **]**

no pgw-address *address* **[s5-s8-protocol pmip]**

no

Removes a previously configured IP address for a P-GW along with the S5 and S8 interface of P-MIP protocol type, and other parameters from this MME service.

address

Specifies the IP address of the P-GW in IPv4 dotted-decimal or IPv6 colon-separated notation.

s5-s8-protocol pmip

Specifies that Proxy-MIP is to be used for S5 and S8 interfaces with the P-GW. By default S5 and S8 interface uses GTP protocol.
pmip Sets the protocol to Proxy-MIP for S5 and S8 interface.

weight *value*

Assigns a weight to the P-GW address to use as a preferred P-GW as an integer from 1 through 100. Lowest value has the least preference.

Usage

Use this command to configure the PDN Gateway (P-GW) addresses to use with MME service. This command also changes the default protocol from GTP to P-MIP for the S5 and S8 interface, and assigns a weight to use when sharing the load between associated P-GWs. A maximum of 16 P-GW addresses can be configured with this command.
This command only changes the use of protocol for the S5 and S8 interface. By default a P-GW uses GTP protocol for S5 and S8 interfaces. This command allows an operator to change the protocol to P-MIP for S5 and S8 interface.
When weight is used, the weights of the operational P-GW(s) are totaled and then weighted round-robin selection is used to distribute new default bearer contexts among P-GW(s).

Important: A maximum of 16 P-GW addresses can be configured per MME service.

Example

The following command associates the P-GW IP address of *192.168.3.1* to the MME service with S5 and S8 protocol as P-MIP and weight as *90*:

```
pgw-address 192.168.3.1 s5-s8-protocol pmip weight 90
```

The following command removes the above configured P-GW IP address and other parameters:

```
no pgw-address 192.168.3.1 s5-s8-protocol pmip
```

plmn-id

Configures the Public Land Mobile Network (PLMN) identifier for this MME service. The PLMN identifier consists of the Mobile Country Code (MCC) and Mobile Network Code (MNC). A single PLMN ID can be configured per MME service.

Product

MME

Privilege

Administrator

Syntax

plmn-id mcc *mcc_value* **mnc** *mnc_value*

no plmn-id mcc *mcc_value* **mnc** *mnc_value*

no

Removes the configured PLMN identifier for this MME service.

Caution: Removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

mcc *mcc_value*

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

mnc *mnc_value*

Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

Usage

Use this command to set the PLMN identifier for this MME service.

Caution: Changing or removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

One PLMN identifier is supported per MME service.

Important: To configure additional PLMN IDs for this MME service, refer to the **network-sharing** command described in this chapter.

Example

The following command configures the PLMN identifier with MCC value as *102* and MNC value as *20* for this MME service:

```
plmn-id mmc 102 mnc 20
```

policy attach

Configures parameters for the UE Attach procedure.

Product

MME

Privilege

Administrator

Syntax

```
policy attach { imei-query-type { imei | imei-sv | none } [ verify-equipment-identity [
allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency ] ] | set-ue-
time { disable | enable }

default policy attach { imei-query-type | set-ue-time }
```

default

Returns the command to its default setting of **none** for **imei-query-type** and **disabled** for **set-ue-time**.

imei-query-type { imei | imei-sv | none }

Configures the IMEI query type for UE attach.

- **imei**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).
- **none**: Specifies that the MME does not need to query for IMEI or IMEI-SV.

verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]

Specifies that the identification (IMEI or IMEI-SV) of the UE is to be performed by the Equipment Identity Register (EIR) over the S13 interface.

- **allow-on-eca-timeout**: Configures the MME to allow equipment that has timed-out on ECA during the attach procedure.
- **deny-greylisted**: Configures the MME to deny grey-listed equipment during the attach procedure.
- **deny-unknown**: Configures the MME to deny unknown equipment during the attach procedure.
- **verify-emergency**: Configures the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases. This keyword is only supported in release 12.2 and higher.

set-ue-time { disable | enable }

Configures the MME to set the time in the UE during the Attach procedure. Default: **disabled**.

Usage

Use this command to configure various MME settings used during the UE Attach procedure.

Example

The following command configures the MME to query the UE for its IMEI and to verify the UEs equipment identity over the S13 interface with an EIR:

```
policy attach imei-query-type imei verify-equipment-identity
```

policy idle-mode

Configures the user-defined policies of session management for an LTE subscriber in an MME service.

Product

MME

Privilege

Administrator

Syntax

```
policy idle-mode detach { explicit | implicit }

[ default ] policy idle-mode detach
```

default

Sets the policy of idle mode detach for a subscriber to its default behavior as implicit.

idle-mode detach

Configures the IDLE mode Detach behavior of a UE.

detach

Defines the Detach procedure while the UE is in IDLE mode.

explicit

Enables the Explicit Detach while a UE is in IDLE mode. The system will page the UE before Detach procedure is started, and then perform the explicit Detach procedure. Default: disabled

implicit

Enables the Implicit Detach while a UE is in IDLE mode. The system never sends any message to the UE before Detach, and executes the Explicit Detach procedure immediately. Default: Enabled

Usage

Use this command to set the user-defined policies for session management in this MME service.

Example

The following command sets the Idle Mode Detach policy to Explicit for a user in this MME service:

```
policy idle-mode detach explicit
```

policy inter-rat

Enables or disables establishment of indirect data forwarding tunnels for Gn/Gp-based Serving Radio Network Subsystem (SRNS) relocations.

Product

MME

Privilege

Administrator

Syntax

```
policy inter-rat indirect-forwarding-tunnels always

no policy inter-rat indirect-forwarding-tunnels
```

no

Disables the function.

indirect-forwarding-tunnels always

Enables establishment of indirect data forwarding tunnels for Gn/Gp-based SRNS relocations.

Usage

Use this command to enable or disable establishment of indirect data forwarding tunnels for Gn/Gp-based SRNS relocations.

Example

The following command enables establishment of indirect data forwarding tunnels for Gn/Gp-based SRNS relocations:

```
policy inter-rat indirect-forwarding-tunnels always
```

policy network

Configures the MME to indicate to the P-GW that all peer SGSNs support dual-addressing for bearers and, subsequently, dual-addressing must be supported for all IPv4 and IPv6 PDNs. Dual-addressing on SGSNs is based on the UE's capability to support inter-RAT roaming.

Product

MME

Privilege

Administrator

Syntax

```
[ default | no ] policy network dual-addressing-supported
```

default

Returns the command to its default setting of disabled.

no

Removes the ability to send dual-addressing support messaging from the MME to the P-GW.

dual-addressing-supported

Specifies that the MME shall indicate to the P-GW that dual-addressing is supported.

Usage

Use this command to configure the MME to send messaging to the P-GW that indicate that all peer SGSNs support dual-addressing for bearers and, subsequently, dual-addressing must be supported for all IPv4 and IPv6 PDNs.

Important: This command can be used for Pre-release 8 and Release 8 SGSNs.

policy overload

Configures the traffic overload policy to control congestion in this service.

Product

MME

Privilege

Administrator

Syntax

```
policy overload { drop | reject }

default policy overload
```

default

Sets the traffic overload policy action to the fault behavior of Reject.

drop

Specifies that the system is to drop the incoming packets with new session requests to avoid overload on MME node. Default: Disabled

reject

Configures the system to reject the new session/call request and responds with a reject message when the threshold for allowed call sessions is crossed on the MME node. Default: Enabled

Usage

Use this command to set the user-defined policies for new call connection attempts when an MME service is overloaded.
Congestion policies at the service-level can be configured for an individual service. When congestion control functionality is enabled, these policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.

Example

The following command sets the nw call connect policy to reject the new session/call request in an MME service:

```
policy overload reject
```

policy pdn-reconnection

Configures the action by the MME when a PDN connection request to an already connected APN is being processed by the MME service.

Product

MME

Privilege

Administrator

Syntax

```
policy pdn-reconnection { multiple | reject | restart }

[ default ] policy pdn-reconnection
```

default

Sets the policy for PDN reconnection to its default behavior of Reject.

multiple

Allows multiple connections to a PDN with the same APN and PDN Type. In this case, the existing connection is left unchanged, and the MME attempts to establish an additional connection to the PDN. Default: Disabled

reject

Configures the MME to deny or reject the request, by sending a PDN Connection Reject command. This is the default behavior. Default: Enabled

restart

Deletes the existing connection and initiates an attempt to establish a new connection. Default: Disabled

Usage

Use this command to set the user-defined policies for PDN reconnection attempt procedures initiated by a UE in an MME service.
While attached the UE can request connections to PDNs. The PDNs are identified by APN (Access Point Name) and PDN Type (ipv4, ipv6 or ipv4v6).
If the UE requests connection to a PDN for which a connection with the same APN name and PDN type already exists, the MME can: 1) deny or reject the request, by sending a PDN connection reject command; 2) allow multiple connections to a PDN with same APN and PDN Type; or 3) delete the existing connection, and attempt to establish a new connection.

Example

The following command sets the PDN reconnect policy to delete the existing PDN and start the attempt to establish a new connection in an MME service:

```
policy pdn-reconnection restart
```

policy s1-reset

Configures how the MME responds to an S1 interface reset.

Product

MME

Privilege

Administrator

Syntax

```
policy s1-reset { detach-ue | idle-mode-entry }

default policy s1-reset
```

default

Returns the command to its default setting of **idle-mode-entry**.

{ detach-ue | idle-mode-entry }

Specifies the action to perform when the S1 interface is reset.
detach-ue: Specifies that UEs are to be implicitly detached from the service upon S1 interface reset.
idle-mode-entry: Specifies that UEs are to be placed into an idle mode condition during S1 interface reset.

Usage

Use this command to configure how the MME reacts to an S1 interface reset condition.

Example

The following command configures the MME to place UEs into an idle state while the S1 interface is being reset:

```
s1-reset idle-mode-entry
```

policy sctp-down

Configures how the MME responds to a failure of the Stream Control Transmission Protocol (SCTP) connection from the eNodeB.

Product

MME

Privilege

Administrator

Syntax

```
policy sctp-down { detach-ue | idle-mode-entry }

default policy sctp-down
```

default

Returns the command to its default setting of **idle-mode-entry**.

{ detach-ue | idle-mode-entry }

Specifies the action to perform when the SCTP connection from the eNodeB fails.
detach-ue: Specifies that UEs are to be detached from the service upon SCTP failure.
idle-mode-entry: Specifies that UEs are to be placed into an idle mode condition upon SCTP failure.

Usage

Use this command to configure how the MME reacts to an SCTP connection failure condition.

Example

The following command configures the MME to place UEs into an idle state while the SCTP connection from the eNodeB fails:

```
sctp-down idle-mode-entry
```

policy tau

Configures parameters for the tracking area update (TAU) procedure.

Product

MME

Privilege

Administrator

Syntax

```
policy tau { imei-query-type { imei | imei-sv | none } [ verify-equipment-identity [
allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency ] ] | set-ue-
time { disable | enable }

default policy tau { imei-query-type | set-ue-time }
```

default

Returns the command to its default setting of **none** for **imei-query-type** and **disabled** for **set-ue-time**.

imei-query-type { imei | imei-sv | none }

Configures the IMEI query type for TAUs.

- **imei**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).
- **none**: Specifies that the MME does not need to query for IMEI or IMEI-SV.

verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]

Specifies that the identification (IMEI or IMEI-SV) of the UE is to be performed by the Equipment Identity Register (EIR) over the S13 interface.

- **allow-on-eca-timeout**: Configures the MME to allow equipment that has timed-out on ECA during the attach procedure.
- **deny-greylisted**: Configures the MME to deny grey-listed equipment during the attach procedure.
- **deny-unknown**: Configures the MME to deny unknown equipment during the attach procedure.
- **verify-emergency**: Configures the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases. This keyword is only supported in release 12.2 and higher.

set-ue-time { disable | enable }

Configures the MME to set the time in the UE during the TAU procedure. Default: **disabled**.

Usage

Use this command to configure various MME settings used during the tracking area update (TAU) procedure.

Example

The following command configures the MME to query the UE for its IMEI and to verify the UEs equipment identity over the S13 interface with an EIR:

```
policy tau imei-query-type imei verify-equipment-identity
```

relative-capacity

Configures a relative capacity variable that is sent o the eNodeB for use in selecting an MME in order to load balance the pool.

Product

MME

Privilege

Administrator

Syntax

relative-capacity *number*

default relative-capacity

default

Returns the command to its default setting of 255.

number

Specifies the relative capacity or weight of an MME compared to others in an MME pool as an integer from 0 through 255. Default: 255

Usage

Use this command to configure the relative capacity or weight of this MME in comparison to other MMEs in a pool. This value is sent to the eNodeB in the S1AP S1 SETUP RESPONSE message.
If this value is changed after the S1 interface is initialized, the MME CONFIGURATION UPDATE message is used to update the eNodeB with the change.

Example

The following command sets this MME with a relative capacity or weight of *100*:

```
relative-capacity 100
```

s1-mme ip

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets of a particular 3GPP QoS class over the S1-MME interface.

Product

MME

Privilege

Administrator

Syntax

```
s1-mme ip qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41
| af42 | af43 | be | ef }

default s1-mme ip qos-dscp
```

qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef }

Default: **af11**
Specifies the DSCP for the specified QoS traffic pattern. **qos-dscp** can be configured to any one of the following:
af11: Assured Forwarding 11 per-hop-behavior (PHB)
af12: Assured Forwarding 12 PHB
af13: Assured Forwarding 13 PHB
af21: Assured Forwarding 21 PHB
af22: Assured Forwarding 22 PHB
af23: Assured Forwarding 23 PHB
af31: Assured Forwarding 31 PHB
af32: Assured Forwarding 32 PHB
af33: Assured Forwarding 33 PHB
af41: Assured Forwarding 41 PHB
af42: Assured Forwarding 42 PHB
af43: Assured Forwarding 43 PHB
be: Best effort forwarding PHB
ef: Expedited forwarding PHB

Usage

DSCP levels can be assigned to specific traffic patterns to ensure that data packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the IP header of every subscriber data packet transmitted over the S1-MME interface(s).

Example

The following command sets the DSCP-level for data traffic sent over the S1-MME interface to **af12**:

```
s1-mme ip qos-dscp af12
```

s1-mme sctp port

Configures the source Stream Control Transmission Protocol (SCTP) port that will be used for binding the SCTP socket to communicate with the eNodeB using S1AP with this MME service.

Product

MME

Privilege

Administrator

Syntax

s1-mme sctp port *port_num*

default s1-mme sctp port

default

Sets the SCTP port to the default value of 36412 to communicate with the eNodeBs using S1-MME interface.

port_num

Specifies the SCTP port number to communicate with the eNodeBs using S1-MME interface as an integer from 1 through 65535. Default: 36412

Usage

Use this command to assign the SCTP port with SCTP socket to communicate with the eNodeB using S1AP. Only one SCTP port can be associated with one MME service.

Example

The following command sets the default SCTP port number 699 for to interact with eNodeB using S1AP on S1-MME interface:

```
default s1-mme sctp port
```

setup-timeout

Configures the timeout duration for setting up MME calls in this MME service.

Product

MME

Privilege

Administrator

Syntax

setup-timeout *dur*

default setup-timeout

default

Sets the call setup timeout duration to the default value of 60 seconds.

dur

Specifies the call setup timeout duration (in seconds) for MME calls after which the attempt will be discarded.
dur is an integer from 1 through 10000. Default: 60

Usage

Use this command to configured the timeout duration for setting up an MME call with an MME service. One this timer expires, the call setup procedure will be discarded within this MME service.

Example

The following command sets the default setup timeout duration of 60 seconds for MME calls:

```
default setup-timeout
```

snmp trap

Enables or disables the SNMP trap for S1 interface connection establishment.

Product

MME

Privilege

Administrator

Syntax

```
[ default | no ] snmp trap { s1-initial-establishment | s1-path-establishment }
```

default

Returns the command to its default setting of disabled.

no

Disables the SNMP trap.

s1-initial-establishment

Specifies that the SNMP trap for the initial S1 interface connection establishment is to be enabled or disabled.

s1-path-establishment

Specifies that the SNMP trap for the S1 path establishment is to be enabled or disabled.

Usage

Use this command to enable or disabled the SNMP trap for S1 interface connection establishment.

ue-db

Configures the UE database that is maintained by the MME as a cache of EPS contexts per UE keyed by IMSI/GUTI to allow the UE to attach by a Globally Unique Temporary Identity (GUTI) and reuse previously established security parameters. This cache will be maintained in each session manager where the first attach occurred for the UE.

Product

MME

Privilege

Administrator

Syntax

ue-db purge-timeout *dur_mins*

default ue-db purge-timeout

default

Resets the UE database purge timer timeout to the default value of 10080 minutes.

purge-timeout *dur_mins*

Sets the timeout duration (in minutes) for MME to store the UE database in cache memory. This timer starts when the UE goes dormant.
dur_mins is an integer from 1 through 20160. Default: 10080

Usage

Use this command to set timeout duration for MME to hold UE database information in cache memory. The MME DB acts as a cache for storing subscriber related information. This subscriber related information helps reduce signaling traffic. The MME DB is a part of the Session Manager and interfaces between the Session Manager Application and Evolved Mobility Management Manager to provide access to the cached data.

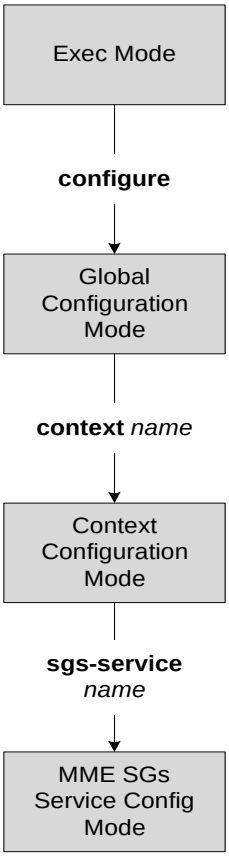
Example

The following command configures the MME database cache timer to hold the UE information up to 7 days (10080 minutes) in the MME Database:

```
default ue-db purge-timeout
```

Chapter 191
MME SGs Service Configuration Mode Commands

The MME SGs Service Configuration Mode is used to create and manage the LTE Mobility Management Entity (MME) SGs services on this system. The SGs service creates an SGs interface between the MME and a Mobile Switching Center/Visitor Location Register (MSC/VLR).



associate

Associates or disassociates a Stream Control Transmission Protocol (SCTP) parameter template with the SGs service.

Product

MME

Privilege

Administrator

Syntax

associate sctp-param-template *template_name*

no associate sctp-param-template

no

template_name

Associates an SCTP parameter template with the SGs service.
template_name specifies the name for a pre-configured SCTP parameter template to associate with this SGs service as an alphanumeric string of 1 through 63 characters. For more information on the SCTP parameter template, refer to the **sctp-param-template** command in the *Global Configuration Mode Commands* chapter and the *SCTP Parameter Template Configuration Mode Commands* chapter.

Usage

Use this command to associate a pre-configured SCTP parameter template with the SGs service.

Important: If no SCTP parameter template is specified, all default settings for the configurable parameters in the SCTP Parameter Template Configuration Mode apply.

Example

The following command associates a pre-configured SCTP parameter template called *sctp-3* to the SGs service:

```
associate sctp-param-template sctp-3
```

bind

Binds the service to a logical IP interface serving as the SGs interface.

Product

MME

Privilege

Administrator

Syntax

bind { ipv4-address *ipv4_address* **[ipv4-address** *ipv4_address* **] | ipv6-address** *ipv6_address* **[ipv6-address** *ipv6_address* **] }**

no bind

no bind

Removes the interface binding from this service.

ipv4-address *ipv4_address* **[ipv4-address** *ipv4_address* **]**

Specifies the IP address of the SGs interface in IPv4 dotted-decimal notation. n.
A secondary IPv4 address can be configured to support SCTP multi-homing.

ipv6-address *ipv6_address* **[ipv6-address** *ipv6_address* **]**

Specifies the IP address of the SGs interface in IPv6 colon-separated notation.
A secondary IPv6 address can be configured to support SCTP multi-homing.

Usage

Associate the SGs service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an SGs interface that provides the session connectivity for circuit switched fallback (CSFB) to/from a Mobile Switching Center/Visitor Location Register (MSC/VLR). Only one interface can be bound to a service. The interface should be configured prior to issuing this command

Example

The following command binds the logical IP interface with the IPv4 address of *192.68.10.22* to the SGs service:

```
bind ipv4-address 192.68.10.22
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

non-pool-area

Configures a non-pool area where a group of Location Area Code (LAC) values use a specific visitor Location Register (VLR).

Product

MME

Privilege

Administrator

Syntax

non-pool-area *name* **use-vlr** *vlr_name* **[lac** *value(s)* **] [plmnid { any | mcc** *mcc_value* **mnc** *mnc_value* **}]**

no non-pool-area *name* **[lac** *value(s)* **]**

no non-pool-area *name* **[lac** *value(s)* **]**

Removes the configured non-pool-area from this service. Optionally, removes a specific LAC or LACs from this non-pool area. *name* is the name of an existing non-pool-area expressed as an alphanumeric string of 1 through 63 characters. *value(s)* is an existing LAC integer value from 1 through 65535.

name

Specifies the name of the non-pool area as an alphanumeric string of 1 through 63 characters.

use-vlr *vlr_name*

Specifies the VLR to be used in this non-pool area configuration as an alphanumeric string of 1 through 63 characters.

lac *value(s)*

Specifies the location area code or codes to be used with the configured VLR in this non-pool area configuration. *value(s)* is an integer(s) from 1 through 65535. A total of 16 area codes can be added in a single line or separately.

plmnid { any | mcc *mcc_value* **mnc** *mnc_value* **}**

Specifies the Public Land Mobile Network (PLMN) identifier to be used with the VLR in this non-pool area configuration.
any: Specifies that any PLMN ID can be used with the VLR in this configuration.
mcc *mcc_value* **mnc** *mnc_value*: Specifies the mobile country code (MCC) and mobile network code (MNC) of the PLMN identifier. *mcc_value* must be an integer from 101 through 998. *mnc_value* must be a 2- or 3-digit integer from 00 through 998.

Usage

Use this command to configure a non-pool area where LAC values and/or PLMN IDs are associated with a specific VLR.

Example

The following command creates a non-pool area named *svlr1* associated with a VLR named *vlr1* and containing LAC values of 1, 2, 3, 4, 5, 6, 7, and 8:

```
non-pool-area svlr1 use-vlr vlr1 lac 1 2 3 4 5 6 7 8
```

pool-area

Creates a location area code (LAC) pool area configuration or specifies an existing pool area and enters the LAC Pool Area Configuration Mode.

Product

MME

Privilege

Administrator

Syntax

[no] pool-area *pool_name* **[-noconfirm]**

no

Removes the selected pool area configuration from the SGs service.

pool_name

Specifies the name of the LAC pool area configuration. If *pool_name* does not refer to an existing pool, a new pool is created. *pool_name* must be an alphanumeric string of 1 through 64 characters.

Important: A total of eight pool areas can be configured per SGs service.

Usage

Use this command to enter the LAC Pool Area Configuration Mode for an existing pool area configuration or for a newly defined pool area configuration. This command is also used to remove an existing pool area configuration.
Entering this command results in the following prompt:

```
[context_name]hostname(config-sgs-pool-area)#
```

LAC Pool Area Configuration Mode commands are defined in the *MME LAC Pool Area Configuration Mode Commands* chapter.

Example

The following command enters the LAC Pool Area Configuration Mode for a new or existing pool area configuration named *pool1*:

```
pool-area pool1
```

sctp

Configures the Stream Control Transmission Protocol (SCTP) port number for this service.

Product

MME

Privilege

Administrator

Syntax

sctp port *port_number*

no sctp

no

Removes the SCTP configuration for this service.

port *port_number*

Specifies the SCTP port number used to communicate with the MSC/VLR using the SGs interface as an integer from 1 through 65535.

Usage

Use this command to assign the SCTP port with SCTP socket to communicate with the MSC/VLR through the SGs interface. A maximum of one SCTP port can be associated with one SGs service.

Example

The following command sets the SCTP port to *29118* for this service:

```
sctp port 29118
```

tac-to-lac-mapping

Maps any Tracking Area Code (TAC) value or a specific TAC value to a LAC value.

Product

MME

Privilege

Administrator

Syntax

```
tac-to-lac-mapping { any-tac | tac value } map-to lac value +

no tac-to-lac-mapping { any-tac | { tac value } + }
```

any-tac | tac *value*

Specifies the TAC to map to the LAC.
any-tac: Specifies that any TAC value is to be mapped to the specified LAC.
tac *value*: Maps a specific TAC value to a LAC value expressed as an integer from 1 through 65535. For specific TAC values, multiple mappings can be entered on the same line (see Example).

map-to lac *value*

Specifies the LAC value that the selected TAC value, or any TAC value is mapped as an integer from 1 through 65535. For specific TAC values, multiple mappings can be entered on the same line (see Example).

Usage

Use this command to map TAC values to LAC values.
Enter up to eight mappings per line. A maximum of 256 mappings can be entered.
If no mapping is entered, the default behavior is TAC equals LAC.

Example

The following command maps a TAC value of 2 to a LAC value of 3, a TAC value of 4 to a LAC value of 5, and a TAC value of 6 to a LAC value of 7:

```
tac-to-lac-mapping tac 2 map-to lac 3 tac 4 map-to lac 5 tac 6 map-to lac
7
```

timer

Configures the SGs-AP Ts6-1 timer value used to guard the Location Update procedure.

Product

MME

Privilege

Administrator

Syntax

timer ts6-1 *value*

default timer ts6-1

default

Returns the command to its default setting of 15.

value

Specifies the Ts6-1 timer value (in seconds) as an integer from 10 through 90. Default: 15

Usage

Use this command to manually set the Ts6-1 timer.

Example

The following command sets the SGs-AP Ts6-1 timer to 20 seconds:

```
timer ts6-1 20
```

vlr

Configures the Visitor Location Register (VLR) to be used by this service.

Product

MME

Privilege

Administrator

Syntax

vlr *vlr_name* **{ ipv4-address** *ipv4_address* **[ipv4-address** *ipv4_address* **] | ipv6-address** *ipv6_address* **[ipv6-address** *ipv6_address* **] } port** *port_number*

no vlr *vlr_name*

no

Removes the configured VLR from this service.

vlr_name

Specifies the name of the VLR as an alphanumeric string of 1 through 63 characters.

ipv4-address *ipv4_address* **[ipv4-address** *ipv4_address* **]**

Specifies the IP address of the VLR in IPv4 dotted-decimal notation.
A secondary IPv4 address can be configured to support SCTP multi-homing.

ipv6-address *ipv6_address* **[ipv6-address** *ipv6_address* **]**

Specifies the IPv6 address of the VLR. *ipv6_address* must be entered in colon-separated notation.
A secondary IPv6 address can be configured to support SCTP multi-homing.

port *port_number*

Specifies the port number of the VLR as an integer from 1 through 65535.

Usage

Use this command to configure the VLR used by this SGs service. A maximum of 32 VLRs can be created.

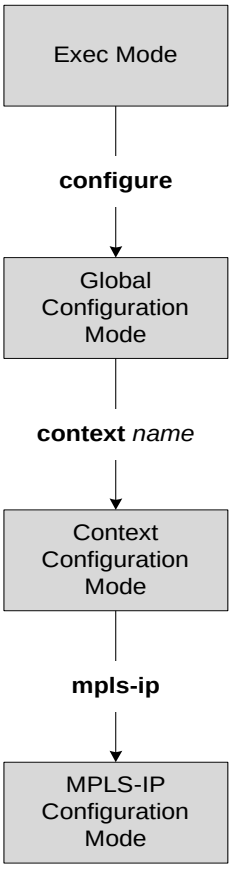
Example

The following command configures a VLR to be used by this service with a name of *vlr1*, an IPv4 address of *10.2.3.4*, and a port number of *29118*:

```
vlr vlr1 ipv4 address 10.2.3.4 port 29118
```

Chapter 192
MPLS-IP Configuration Mode Commands

The MPLS-IP Configuration Mode is used for configuration of Multiprotocol Label Switching (MPLS) IP forwarding specific parameters. This mode is entered from the Context Configuration Mode.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

protocol

This command creates or removes the MPLS protocol family configuration modes, or configures an existing protocol and enters the MPLS-LDP Configuration Mode in the current context. This command configures the protocol parameters for the MPLS protocol family.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[no] protocol ldp
```

no

Removes the configured MPLS-LDP mode from MPLS-IP Configuration mode.

ldp

Specifies the type of MPLS protocol to LDP and creates/enters the MPLS-LDP Configuration Mode for Label Distribution Protocol (LDP) specific configuration in an MPLS-IP configuration instance.

Usage

Use this command to create/ or remove the MPLS protocol family configuration mode, or configure an existing protocol. If required mode already exists it enters the MPLS-LDP Configuration Mode in the current context.
Entering this command results in the following prompt:

```
[context_name]hostname(config-ldp)#
```

The commands configured in this mode are defined in the *MPLS-LDP Configuration Mode Commands* chapter.

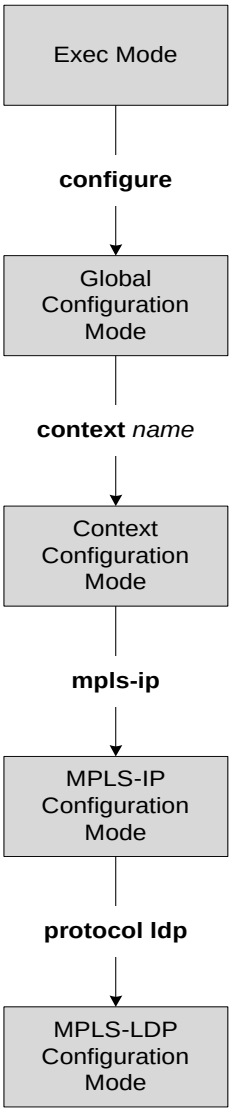
Example

The following command creates and enters the MPLS-LDP Protocol mode for Label Distribution Protocol parameters in MPLS-IP Configuration instance:

```
protocol ldp
```

Chapter 193
MPLS-LDP Configuration Mode Commands

The MPLS-LDP Configuration Mode is used to configure Label Distribution Protocol (LDP) specific parameters for MPLS-IP forwarding.



advertise-labels

Configures the Label Advertisement parameters.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[no] advertise-labels { explicit-null | implicit-null }

default advertise-labels
```

no

Disables the label advertisement parameters.

default

Advertises the labels from the label space allocated for LDP protocol.

explicit-null

Advertises the Explicit NULL label for all the prefixes.

implicit-null

Advertises the Implicit NULL label for all the prefixes.

Usage

Use this to configure advertisement of the Implicit NULL or Explicit NULL label for all the prefixes advertised by the system in this context.

Example

The following command configures the MPLS-IP forwarding to advertise the Explicit NULL label for all the prefixes:

```
advertise-labels explicit-null
```

The following command configures the MPLS-IP forwarding to advertise the Implicit NULL label for all the prefixes:

```
advertise-labels implicit-null
```

discovery

Configures the Label Distribution Protocol (LDP) neighbor discovery parameters.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
discovery { hello { hello-interval integer_value | hold-interval integer_value } |
transport-address ipv4_addr }

default discovery hello

no discovery transport-address
```

default

Sets the LDP discovery hello interval at 5 seconds and hold interval at 15 seconds.

no

Disables the LDP neighbor discovery.

hello { hello-interval *integer_value* **| hold-interval** *integer_value* **}**

Configures the LDP Hello parameters.
hello-interval configures the frequency of sending the Discovery Hello packets in seconds.
integer_value is an integer from 5 through 21845.
Default: 5
hold-interval configures the Discovery Hold time interval in seconds.
integer_value is an integer from 15 through 65535.
Default: 15

transport-address *ipv4_addr*

Configures the LDP transport address as an IPv4 address entered in dotted-decimal notation. Transport address is the same as the LDP router ID.

Usage

This is an optional command that is used to configure LDP peer discovery parameters. The LDP discovery hold-interval is always set to three times the LDP discovery hello-interval. Transport address is the address used for the TCP session over which LDP is running. If the transport address is not configured, the LDP router-id is used as transport address. Any update to transport address will take effect only if LDP is disabled and re-enabled. The “default” option sets the hello intervals to the default values.

Example

The following command sequence configures the LDP peer discovery parameters:

```
discovery hello hello-interval 10discovery hello hold-interval
30discovery transport-address 10.2.3.4
```

enable

Enables the Label Distribution Protocol (LDP).

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] enable
```

no

Disables the LDP protocol.

Usage

This command is used to enable or disable the LDP protocol. By default the LDP protocol is disabled.

Example

Use the following command to enable the LDP protocol:

```
enable
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

router-id

Configures the Label Distribution Protocol Router ID.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

router-id *ipv4_addr*
no router-id

no

Disables the router ID.

ipv4_addr

Must be an IPv4 address entered in dotted-decimal notation.

Usage

This command is used to configure the LDP router-id. This is an optional parameter. If the ID is not configured, the largest operational loopback address is selected as the LDP router ID. If LDP has started, any change will take effect only after disabling and enabling LDP.

Example

The following command sequence configures an LDP router ID:

```
router-id 10.2.3.4
```

session

Configures the LDP session parameters.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
session timers { hold-interval integer_value | keepalive-interval integer_value }
default session timers
```

default

Configures the default values for hold-interval parameter at 45 and keepalive-interval parameter at 15.

timers

Configures the LDP session keepalive parameters.

hold-interval *integer_value*

Configures the session hold time interval in seconds.
integer_value is an integer from 45 through 65535.
Default: 45

keepalive-interval *integer_value*

Configures the frequency of sending keepalive packets in seconds.
integer_value is an integer from 15 through 21845.
Default: 15

Usage

This optional command is used to configure LDP session timers. LDP session hold-interval is always set to three times the LDP session keepalive-interval. The “default” option sets the session keepalive and hold intervals to the default values.

Example

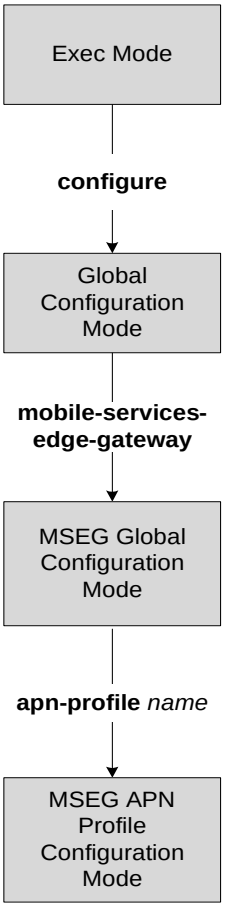
The following command sequence configures the LDP session parameters:

```
session timers keepalive-interval 30

session timers hold-interval 45

default session timers
```

Chapter 194
MSEG APN Profile Configuration Mode Commands

The MSEG APN Profile Configuration Mode allows you to configure Access Point Name(s) (APN) in a Mobile Service Edge Gateway (MSEG) APN profile.

Important: This configuration mode is not supported in this release. For more information please contact your Cisco account representative.



apn

This command allows you to add/remove APN names from an MSEG APN profile.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

[no] apn *apn_name*

no

If previously configured, deletes the specified APN name in the current MSEG APN profile.

apn_name

Specifies the APN to add/remove.
apn_name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to add/remove APN names from an MSEG APN profile.
The APN names configured in the APN profile are wild-cardable strings that are used to match against the APN name in the incoming CPC requests for offload eligibility. APN names are one of the level-one MSEG filters.
Multiple APN names can be configured in each APN profile to form sets of APN names.

Example

The following command adds the APN named *test* to the current APN profile:

```
apn test
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

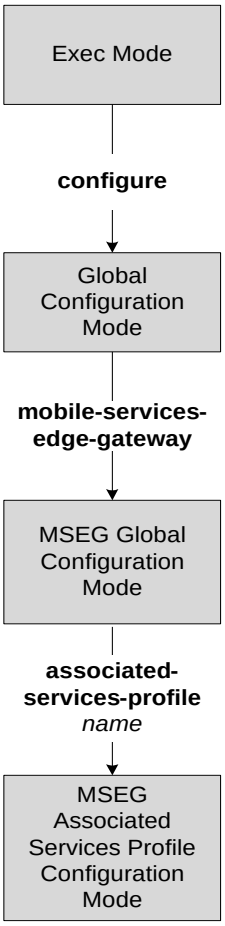
Usage

Use this command to return to the parent configuration mode.

Chapter 195
MSEG Associated Services Profile Configuration Mode Commands

The MSEG Associated Services Profile Configuration Mode enables you to configure the associated services, such as NAT, accounting context, and destination context, that must be applied to an off-loaded session once it is set up.

Important: This configuration mode is not supported in this release. For more information please contact your Cisco account representative.



active-charging-rulebase

This command allows you to configure an ACS rulebase in the MSEG associated services profile.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

active-charging-rulebase *acs_rulebase_name*

no active-charging-rulebase

no

If previously configured, deletes the ACS rulebase from the current MSEG associated services profile.

acs_rulebase_name

Specifies the ACS rulebase.
acs_rulebase_name must be the name of an ACS rulebase, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure an ACS rulebase in the MSEG associated services profile. By default, there is no ACS rulebase configured in a profile.
Rulebase configuration is used in the ACS context for configuring collection of rule definitions and their associated billing policy. Different rulebases can be configured for different set of subscribers by defining appropriate MSEG filters.

Example

The following command configures an ACS rulebase named *test* in the current MSEG associated services profile:

```
active-charging-rulebase test
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

fw-nat-policy

This command allows you to configure a Firewall-and-NAT policy in the MSEG associated services profile.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

fw-nat-policy *fw_nat_policy_name*

no fw-nat-policy

no

If previously configured, deletes the Firewall-and-NAT policy from the current MSEG associated services profile.

fw_nat_policy_name

Specifies the Firewall-and-NAT policy.
fw_nat_policy_name must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure a Firewall-and-NAT policy in the MSEG associated services profile. By default, there is no Firewall-and-NAT policy configured in a profile.
If, in the profile, an ACS rulebase is configured and there is a Firewall-and-NAT policy configured in that rulebase, the Firewall-and-NAT policy configured using this command will take precedence for sessions that are offloaded. If not configured, the MSEG will act as an anchor-proxy for the offloaded calls.

Example

The following command configures a Firewall-and-NAT policy named *test* in the current MSEG associated services profile:

```
fw-nat-policy test
```

ip

This command allows you to configure IP parameters in the MSEG associated services profile.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

ip { access-group *access_group_name* **{ in | out } | context-name** *context_name* **}**

no ip { access-group { in | out } | context-name }

no

If previously configured, deletes the specified IP configuration from the current MSEG associated services profile.

access-group *access_group_name* **{ in | out }**

Specifies the IPv4/IPv6 access group to use for redirecting traffic to the ACS subsystem.
access_group_name must be the name of an IPv4/IPv6 access group, and must be an alphanumeric string of 1 through 63 characters.
in specifies that the ACL group be applied to inbound traffic.
out specifies that the ACL group be applied to outbound traffic.

context-name *context_name*

Specifies the destination context to use.
context_name must be the name of the destination context, must be an alphanumeric string of 1 through 63 characters.

Important: If the context name is not configured, MSEG service context will be used.

Usage

Use this command to configure IP parameters in an MSEG associated services profile. The IPv4/IPv6 access group is used for redirecting the traffic to ACS Subsystem.

Example

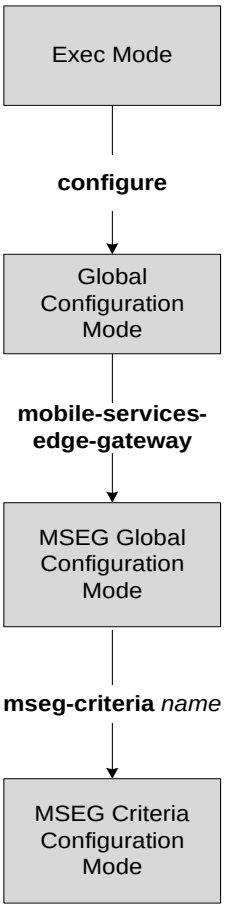
The following command configures the IP access group named *test* to be applied on outbound traffic in the current MSEG associated services profile:

```
ip access-group test out
```

Chapter 196
MSEG Criteria Configuration Mode Commands

The MSEG Criteria Configuration Mode enables you to configure a set of MSEG filters that are applied by an MSEG service. There can be multiple MSEG criteria configured, but only one can be associated with any MSEG service at any given time.

Important: This configuration mode is not supported in this release. For more information please contact your Cisco account representative.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

filter priority

This command allows you to add/configure/delete filters in an MSEG criteria.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

filter priority *priority* **ruleset** *ruleset_name* **action { forward | local-terminate | offload associated-services-profile** *profile_name* **}**

no filter priority *priority*

no

Deletes the specified filter from the current offload criteria.

priority

Specifies the priority of the filter.
priority must be an integer from 1 through 10.

ruleset *ruleset_name*

Specifies the ruleset.
ruleset_name must be the name of a ruleset, and must be an alphanumeric string of 1 through 63 characters.

action { forward | local-terminate | offload associated-services-profile *profile_name* **}**

Specifies the action to apply.

- **forward**: Specifies to forward to GGSN.

  The CPC request will be forwarded to the actual GGSN without any further processing by MSEG. Thus, the MSEG will remove itself from the path for that PDP session. This action is applicable only to the primary PDP context setup.

- **local-terminate**: Specifies to terminate locally at MSEG.

  The CPC request will be forwarded to a co-located GGSN service for anchoring. The MSEG will subsequently not be in the path of the CPC setup. This action is applicable only to the primary PDP context setup.

- **offload associated-services-profile** *profile_name*: Specifies to offload the PDP session at MSEG, the specified associated service profile will be applicable.

profile_name must be the name of an associated service profile, and must be an alpha and/or numeric string of 1 through 63 characters in length.

If the NAT configuration has not been enabled in the associated service profile, only the proxy-anchor mode will be applicable for the call. That is, all data will be tunneled to the anchor GGSN instead of being locally offloaded via NAT. This will be the default behavior for all offloaded calls and can be overridden by specifying local-breakout for the data-plane by associating NAT configuration.

Usage

Use this command to add/configure/remove filters in an offload criteria.
There can be multiple offload criteria configured though only one can be associated with an MSEG service at any given time. The filters will be processed in ascending order of priority, and the action corresponding to the first match will be applied.

Example

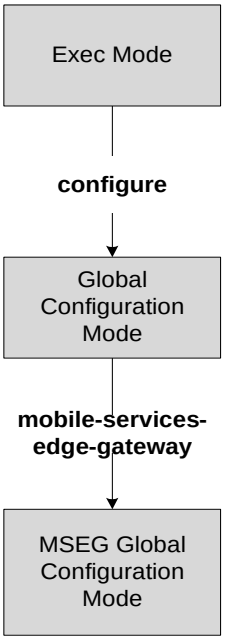
The following command configures an offload filter to offload PDP session with the filter's priority set to *1*, the ruleset named *test_ruleset*, the services profile named *test_profile*:

```
filter priority 1 ruleset test_ruleset action offload associated-
services-profile test_profile
```

Chapter 197
MSEG Global Configuration Mode Commands

The MSEG Global Configuration Mode is used to configure global Mobile Service Edge Gateway (MSEG) parameters.

Important: This configuration mode is not supported in this release. For more information please contact your Cisco account representative.



apn-profile

This command allows you to create/configure/delete MSEG APN profiles.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

apn-profile *mseg_apn_profile_name* **[-noconfirm]**

no apn-profile *mseg_apn_profile_name*

no

Deletes the specified MSEG APN profile.

mseg_apn_profile_name

Specifies the APN profile to add/configure/delete.
mseg_apn_profile_name must be the name of an MSEG APN profile, and must be an alphanumeric string of 1 through 63 characters.
If the named APN profile does not exist, it is created, and the CLI mode changes to the MSEG APN Profile Configuration Mode wherein the APN profile can be configured.
If the named APN profile already exists, the CLI mode changes to the MSEG APN Profile Configuration mode for that APN profile.

-noconfirm

Executes the command without prompting for confirmation.

Usage

Use this command to create/configure/delete MSEG APN profiles.
Entering this command results in the following prompt:
`[context_name]hostname(config-mseg-apn-profile)#`
MSEG APN Profile configuration commands are described in the *MSEG APN Profile Configuration Mode Commands* chapter.

Example

The following command creates an APN profile named *test*, and changes to the MSEG APN Profile Configuration Mode:

```
apn-profile test
```

associated-services-profile

This command allows you to create/configure/delete MSEG associated-services profiles.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

associated-services-profile *mseg_as_profile_name* **[-noconfirm]**

no associated-services-profile *mseg_as_profile_name*

no

Deletes the specified MSEG associated-services profile.

mseg_as_profile_name

Specifies the MSEG associated services profile to add/configure/delete.
mseg_as_profile_name must be the name of an MSEG associated-services profile, and must be an alphanumeric string of 1 through 63 characters.
If the named associated-services profile does not exist, it is created, and the CLI mode changes to the MSEG Associated Services Profile Configuration Mode wherein the profile can be configured.
If the named associated-services profile already exists, the CLI mode changes to the MSEG Associated Services Profile Configuration Mode for that profile.

-noconfirm

Executes the command without prompting for confirmation.

Usage

Use this command to create/configure/delete MSEG associated-services profiles.
Entering this command results in the following prompt:
`[context_name]hostname(config-mseg-as-profile)#`
MSEG associated-services profile configuration commands are described in the *MSEG Associated Services Profile Configuration Mode Commands* chapter. This mode contains configurations for all the associated services such as NAT, accounting context, destination context, and so on, from other parts of the system, that are to be applied to an offloaded session once it is set up.

Example

The following command creates an associated-services profile named *test*, and changes to the MSEG Associated Services Profile Configuration Mode:

```
associated-services-profile test
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

imei-profile

This command allows you to create/configure/delete MSEG IMEI profiles.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

imei-profile *mseg_imei_profile_name* **[-noconfirm]**

no imei-profile *mseg_imei_profile_name*

no

Deletes the specified MSEG IMEI profile.

mseg_imei_profile_name

Specifies the MSEG IMEI profile to add/configure/delete.
mseg_imei_profile_name must be the name of an MSEG IMEI profile, and must be an alphanumeric string of 1 through 63 characters.
If the named IMEI profile does not exist, it is created, and the CLI mode changes to the MSEG IMEI Profile Configuration Mode wherein the IMEI profile can be configured.
If the named IMEI profile already exists, the CLI mode changes to the MSEG IMEI Profile Configuration Mode for that IMEI profile.

-noconfirm

Executes the command without prompting for confirmation.

Usage

Use this command to create/configure/delete MSEG IMEI profiles.
Entering this command results in the following prompt:
`[context_name]hostname(config-mseg-imei-profile)#`
MSEG IMEI Profile configuration commands are described in the *MSEG IMEI Profile Configuration Mode Commands* chapter.

Example

The following command creates an IMEI profile named *test*, and changes to the MSEG IMEI Profile Configuration Mode:

```
imei-profile test
```

imsi-profile

This command allows you to create/configure/delete MSEG IMSI profiles.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

imsi-profile *mseg_imsi_profile_name* **[-noconfirm]**

no imsi-profile *mseg_imsi_profile_name*

no

Deletes the specified MSEG IMSI profile.

mseg_imsi_profile_name

Specifies the MSEG IMSI profile to add/configure/delete.
mseg_imsi_profile_name must be the name of an MSEG IMSI profile, and must be an alphanumeric string of 1 through 63 characters.
If the named IMSI profile does not exist, it is created, and the CLI mode changes to the MSEG IMSI Profile Configuration Mode wherein the IMSI profile can be configured.
If the named IMSI profile already exists, the CLI mode changes to the MSEG IMSI Profile Configuration Mode for that IMSI profile.

-noconfirm

Executes the command without prompting for confirmation.

Usage

Use this command to create/configure/delete MSEG IMSI profiles.
Entering this command results in the following prompt:
`[context_name]hostname(config-mseg-imsi-profile)#`
MSEG IMSI Profile configuration commands are described in the *MSEG IMSI Profile Configuration Mode Commands* chapter.

Example

The following command creates an IMSI profile named *test*, and changes to the MSEG IMSI Profile Configuration Mode:

```
imsi-profile test
```

mseg-criteria

This command allows you to create/configure/delete MSEG criteria.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

mseg-criteria *mseg_criteria_name* **[-noconfirm]**

no mseg-criteria *mseg_criteria_name*

no

Deletes the specified MSEG criteria.

mseg_criteria_name

Specifies the MSEG criteria to add/configure/delete.
mseg_criteria_name must be the name of the MSEG criteria, and must be an alphanumeric string of 1 through 63 characters.
If the named MSEG criteria does not exist, it is created, and the CLI mode changes to the MSEG Criteria Configuration Mode wherein the MSEG criteria set can be configured.
If the named MSEG criteria already exists, the CLI mode changes to the MSEG Criteria Configuration Mode for that MSEG criteria.

-noconfirm

Executes the command without prompting for confirmation.

Usage

Use this command to create/configure/delete an MSEG criteria — a set of filters that are applied by an MSEG service. There can be multiple MSEG criteria configured though only one can be associated with an MSEG service at any given time.
Entering this command results in the following prompt:
`[context_name]hostname(config-mseg-criteria)#`
MSEG criteria configuration commands are described in the *MSEG Criteria Configuration Mode Commands* chapter.

Example

The following command creates an MSEG criteria named *test*, and changes to the MSEG Criteria Configuration Mode:

```
mseg-criteria test
```

mseg-ruleset

This command allows you to create/configure/delete MSEG rules.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

mseg-ruleset *mseg_ruleset_name* **[-noconfirm]**

no mseg-ruleset *mseg_ruleset_name*

no

Deletes the specified MSEG ruleset.

mseg_ruleset_name

Specifies the MSEG ruleset to add/configure/delete.
mseg_ruleset_name must be the name of an MSEG ruleset, and must be an alphanumeric string of 1 through 63 characters.
If the named MSEG ruleset does not exist, it is created, and the CLI mode changes to the MSEG Ruleset Configuration Mode wherein the MSEG ruleset can be configured.
If the named MSEG ruleset already exists, the CLI mode changes to the MSEG Ruleset Configuration Mode for that MSEG ruleset.

-noconfirm

Executes the command without prompting for confirmation.

Usage

Use this command to create/configure/delete MSEG rulesets — filter combinations to be applied while evaluating whether a session should be offloaded or not.
Entering this command results in the following prompt:
`[context_name]hostname(config-mseg-ruleset)#`
MSEG ruleset configuration commands are described in the *MSEG Ruleset Configuration Mode Commands* chapter.

Example

The following command creates an MSEG ruleset named *test*, and changes to the MSEG Ruleset Configuration Mode:

```
mseg-ruleset test
```

peer-mseg-profile

This command allows you to create/configure/delete MSEG peer profiles.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

peer-mseg-profile *mseg_peer_profile_name* **[-noconfirm]**

no peer-mseg-profile *mseg_peer_profile_name*

no

Deletes the specified MSEG peer profile.

mseg_peer_profile_name

Specifies the MSEG peer profile to add/configure/delete.
mseg_peer_profile_name must be the name of an MSEG peer profile, and must be an alphanumeric string of 1 through 63 characters.
If the named MSEG peer profile does not exist, it is created, and the CLI mode changes to the MSEG Peer Profile Configuration Mode wherein the MSEG peer profile can be configured.
If the named MSEG peer profile already exists, the CLI mode changes to the MSEG Peer Profile Configuration Mode for that peer profile.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete MSEG peer profiles. Configuration of all non-local MSEG instances in the network. Multiple MSEG peer profiles can be configured.
Entering this command results in the following prompt:
`[context_name]hostname(config-mseg-profile)#`
MSEG peer profile configuration commands are described in the *MSEG Peer Profile Configuration Mode Commands* chapter.

Example

The following command creates a peer profile named *test*, and changes to the MSEG Peer Profile Configuration Mode:

```
peer-mseg-profile test
```

rnc-profile

This command allows you to create/configure/delete MSEG Radio Network Controller (RNC) profiles.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

rnc-profile *mseg_rnc_profile_name* **[-noconfirm]**

no rnc-profile *mseg_rnc_profile_name*

no

Deletes the specified MSEG RNC profile.

mseg_rnc_profile_name

Specifies the MSEG RNC profile to add/configure/delete.
mseg_rnc_profile_name must be the name of an MSEG RNC profile, and must be an alphanumeric string of 1 through 63 characters.
If the named RNC profile does not exist, it is created, and the CLI mode changes to the MSEG RNC Profile Configuration Mode wherein the RNC profile can be configured.
If the named RNC profile already exists, the CLI mode changes to the MSEG RNC Profile Configuration Mode for that RNC profile.

-noconfirm

Executes the command without prompting for confirmation.

Usage

Use this command to create/configure/delete MSEG RNC profiles. Multiple RNC profiles can be configured.
Entering this command results in the following prompt:
`[context_name]hostname(config-mseg-rnc-profile)#`
MSEG RNC Profile configuration commands are described in the *MSEG RNC Profile Configuration Mode Commands* chapter.

Example

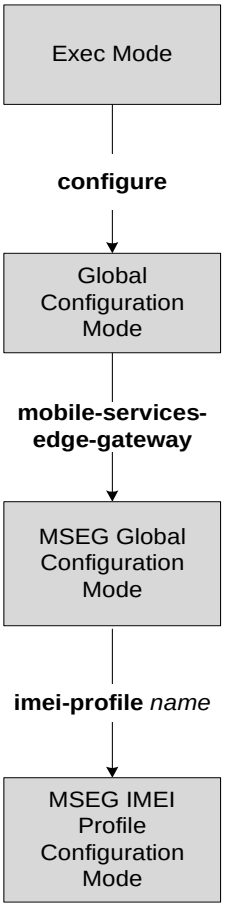
The following command creates an RNC profile named *test*, and changes to the MSEG RNC Profile Configuration Mode:

```
rnc-profile test
```

Chapter 198
MSEG IMEI Profile Configuration Mode Commands

The MSEG IMEI Profile Configuration Mode enables to configure International Mobile Equipment Identifier (IMEI) ranges in Mobile Service Edge Gateway (MSEG) IMEI profiles.

Important: This configuration mode is not supported in this release. For more information please contact your Cisco account representative.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

imei-range

This command allows you to add/remove IMEI ranges in an MSEG IMEI profile.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

[no] imei-range start *imei_prefix_range_start* **end** *imei_prefix_range_end* **[sv** *imei_sw_version* **]**

no

Deletes the specified IMEI prefix range.

start *imei_prefix_range_start*

Specifies the start of the IMEI prefix range as an integer.

end *imei_prefix_range_end*

Specifies the end of the IMEI prefix range as an integer.

sv *imei_sw_version*

Specifies software version of IMEISV as a 2-digit integer.

Usage

Use this command to add/remove IMEI ranges in an MSEG IMEI profile.
Multiple, non-overlapping, IMEI ranges can be specified in each IMEI profile. IMEI ranges are level-one filters.

Example

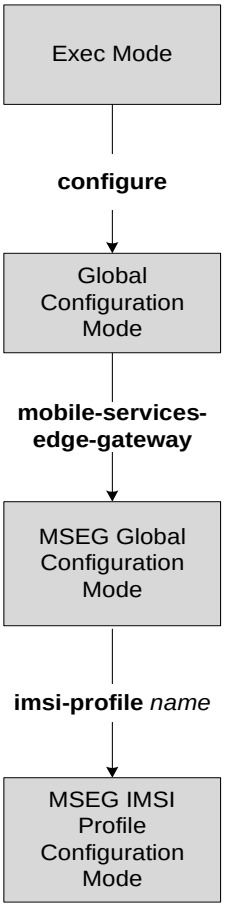
The following command adds an IMEI range starting with the IMEI prefix *123* and ending with the IMEI prefix *456*:

```
imei-range start 123 end 456
```

Chapter 199
MSEG IMSI Profile Configuration Mode Commands

The MSEG IMSI Profile Configuration Mode enables you to configure International Mobile Subscriber Identifier (IMSI) ranges, which are level-1 filters, in Mobile Service Edge Gateway (MSEG) IMSI profiles.

Important: This configuration mode is not supported in this release. For more information please contact your Cisco account representative.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

imsi-range

This command allows you to add/remove IMSI ranges in an MSEG IMSI profile.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

[no] imsi-range mcc *mobile_country_code* **mnc** *mobile_network_code* **msin start** *msin_start* **end** *msin_end*

no

Deletes the specified IMSI range.

mcc *mobile_country_code*

Specifies the Mobile Country Code (MCC) of IMSI as an integer from 100 through 999.
Note that MCC values 000 through 099 are reserved codes.

mnc *mobile_network_code*

Specifies the Mobile Network Code (MNC) of IMSI as a 2- or 3-digit integer from 00 through 999.

msin start *msin_start* **end** *msin_end*

Specifies the Mobile Subscriber International Number (MSIN) range.
msin start *msin_start*: Specifies the start of the MSIN prefix range as an integer.
end *msin_end*: Specifies the end of the MSIN prefix range as an integer.

Usage

Use this command to add/remove IMSI ranges in an MSEG IMSI profile.
Multiple, non-overlapping, IMSI ranges can be specified in each IMSI profile.

Example

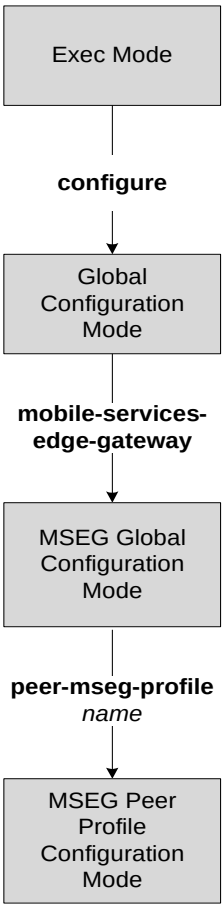
The following command adds an IMSI range to the current IMSI profile with the MCC and MNC set to *111*:

```
imsi-range mcc 111 mnc 111 msin start 123 end 456
```

Chapter 200
MSEG Peer Profile Configuration Mode Commands

This configuration mode enables you to configure non-local Mobile Service Edge Gateway (MSEG) instances in the network. Though this mode is intended to contain peer-MSEG information, there is no restriction on configuring local MSEG instances. Local MSEG service instances will look up this list and the list of local MSEG services whenever necessary.

Important: This configuration mode is not supported in this release. For more information please contact your Cisco account representative.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

mseg-gtpc

This command allows you to add/remove MSEG service control addresses in an MSEG peer profile.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

mseg-gtpc *ipv4/ipv6_address* **[udp-port** *port_number* **]**

no mseg-gtpc

no

Deletes the previously configured MSEG GTP-C address from the current MSEG peer profile.

ipv4/ipv6_address

Specifies the MSEG GTP-C IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.

udp-port *port_number*

Specifies the UDP port number as an integer from 1 through 65535.

Usage

Use this command to add/remove MSEG service control addresses in an MSEG peer profile.

Example

The following command configures the MSEG GTP-C address *1.1.1.1* and the UDP port *111* in the current MSEG peer profile:

```
mseg-gtpc 1.1.1.1 udp-port 111
```

mseg-gtpu

This command allows you to add/remove MSEG service data addresses in an MSEG peer profile.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

[no] mseg-gtpu *ipv4/ipv6_address*

no

Deletes the specified MSEG GTP-U address from the current MSEG peer profile.

ipv4/ipv6_address

Specifies the MSEG GTP-U IP address in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to add/remove MSEG service data addresses in an MSEG peer profile. Multiple GTP-U addresses can be associated with an MSEG instance.

Example

The following command configures the MSEG GTP-U address *1.1.1.1* for the current MSEG peer profile:

```
mseg-gtpu 1.1.1.1
```

mseg-id

This command allows you to configure the MSEG instance ID in an MSEG peer profile. Note that the MSEG profile is not activated until this ID is configured.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

[no] mseg-id *mseg_id*

no

Deactivates the specified MSEG peer profile.

mseg_id

Specifies the MSEG instance ID as n integer from 1 through 65535.

Usage

Use this command to configure the MSEG instance ID in an MSEG peer profile.
This ID must be unique across all MSEG installations in an operator's domain. The MSEG profile is not activated until this ID is configured.

Example

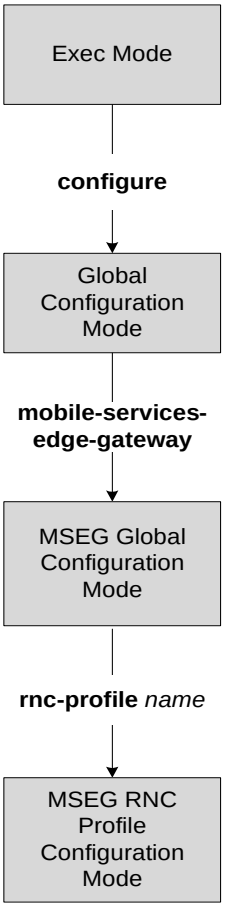
The following command configures the MSEG instance ID in the current MSEG peer profile to *111*:

```
mseg-id 111
```

Chapter 201
MSEG RNC Profile Configuration Mode Commands

The MSEG RNC Profile Configuration Mode enables to configure Mobile Service Edge Gateway (MSEG) Radio Network Controller (RNC) profiles.

Important: This configuration mode is not supported in this release. For more information please contact your Cisco account representative.



associate

This command allows you to configure the MSEG to associate with/serve the RNC.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

`[ no ] associate mseg-profile` *`mseg_profile_name`*

`no`

Disassociates the specified MSEG filter from the RNC.

`mseg_profile_name`

Specifies the name of an MSEG profile as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the MSEG to associate with/serve the RNC.
Only one MSEG can be associated with an RNC.

Example

The following command associates the MSEG named *`test`* with the RNC:

```
associate mseg-profile test
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

location

This command allows you to add/remove locations that the RNC serves in an MSEG RNC profile.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

location mcc *mobile_country_code* **mnc** *mobile_network_code* **lac** *location_area_code* **sac** *service_area_code*

no location

no

Deletes the previously configured location address in the current MSEG RNC profile.

mcc *mobile_country_code*

Specifies the Mobile Country Code (MCC) as an integer from 100 through 999.
Note that MCC values from 000 through 099 are reserved codes.

mnc *mobile_network_code*

Specifies the Mobile Network Code (MNC) as a 2- or 3-digit integer fromv00 through 999.

lac *location_area_code*

Specifies the Location Area Code (LAC) as an integer from 1 through 65535.

sac *service_area_code*

Specifies the Service Area Code (SAC) as an integer from 1 through 65535.

Usage

Use this command to add/remove locations that the RNC serves in an MSEG RNC profile.
Multiple locations can be configured in an MSEG RNC profile.

Example

The following command adds a location address to the current RNC profile with the MCC, MNC, LAC, and SAC set to *111*:

```
location mcc 111 mnc 111 lac 111 sac 111
```

rnc-gtpu

This command allows you to add/remove data addresses associated with the RNC.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

[no] rnc-gtpu *ipv4/ipv6_address* **[udp-port** *port_number* **]**

no

Deletes the specified RNC GTP-U address from the current RNC profile.

ipv4/ipv6_address

Specifies the GTP-U address in IPv4 dotted-decimal or IPv6 colon-separated notation.

udp-port *port_number*

Specifies the UDP port number as an integer from 1 through 65535.

Usage

Use this command to add/remove RNC data addresses associated with the RNC in an MSEG RNC profile. Multiple GTP-U addresses can be associated with the RNC.

Example

The following command configures the RNC GTP-U address *1.1.1.1* and the UDP port *111* in the current MSEG RNC profile:

```
rnc-gtpu 1.1.1.1 udp-port 111
```

rnc-id

This command allows you to configure the RNC ID in an MSEG RNC profile.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

[no] rnc-id *rnc_id*

no

Deletes the specified RNC ID from the current MSEG RNC profile.

rnc_id

Specifies the RNC ID as an integer from 1 through 65535.

Usage

Use this command to configure the RNC ID in an MSEG RNC profile.
Only one RNC ID can be configured in an MSEG RNC profile.

Example

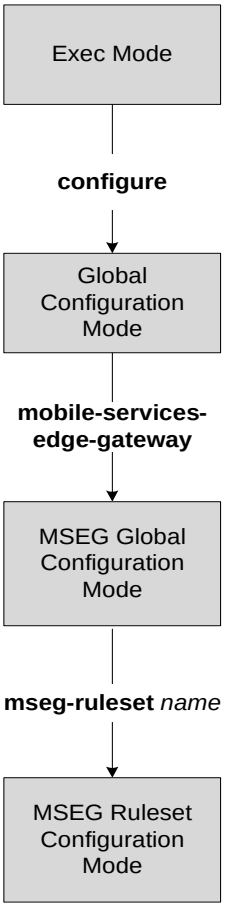
The following command configures the RNC ID *111* in the current MSEG RNC profile:

```
rnc-id 111
```

Chapter 202
MSEG Ruleset Configuration Mode Commands

The MSEG Ruleset Configuration Mode enables you to configure rules to be applied when evaluating whether a session should be offloaded or not.

Important: This configuration mode is not supported in this release. For more information please contact your Cisco account representative.



apn

This command allows you to associate specified APN profile(s) with the rule.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

[no] apn { if-match-profile *apn_profile_name* **| if-no-match-profile** *apn_profile_name* **}**

no

Removes the specified APN rule from the ruleset.

if-match-profile *apn_profile_name*

Specifies name of the APN profile to be applied on match as an alphanumeric string of 1 through 63 characters.

if-no-match-profile *apn_profile_name*

Specifies name of the APN profile to be applied on no match as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to associate APN profile(s) to the rule, and specify which APN profile must be applied if the APN matches/does not match.

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

imei

This command allows you to associate specified International Mobile Equipment Identity (IMEI) profile(s) with the rule.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

[no] imei { if-match-profile *imei_profile_name* **| if-no-match-profile** *imei_profile_name* **}**

no

Removes the specified IMEI rule from the ruleset.

if-match-profile *imei_profile_name*

Specifies name of the IMEI profile to be applied on match as an alphanumeric string of 1 through 63 characters.

if-no-match-profile *imei_profile_name*

Specifies name of the IMEI profile to be applied on no match as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to associate IMEI profile(s) to the rule, and specify which IMEI profile must be applied if the subscriber IMEI matches/does not match.

imsi

This command allows you to associate specified IMSI profile(s) with the rule.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] imsi { if-match-profile imsi_profile_name | if-no-match-profile imsi_profile_name
}
```

no

Removes the specified IMSI rule from the ruleset.

if-match-profile *imsi_profile_name*

Specifies name of the IMSI profile to be applied on match as an alphanumeric string of 1 through 63 characters.

if-no-match-profile *imsi_profile_name*

Specifies name of the IMSI profile to be applied on no match as an alphanumeric string of 1 through 63 characters.

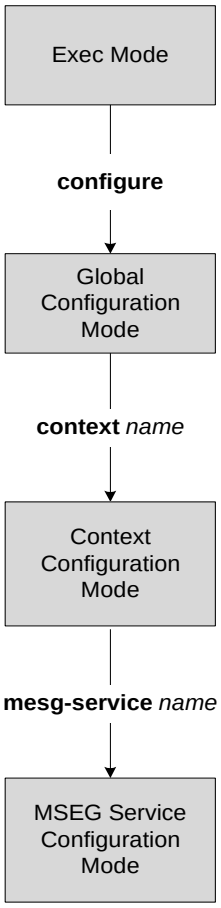
Usage

Use this command to associate IMSI profile(s) to the rule, and specify which IMSI profile must be applied if the subscriber IMSI matches/does not match.

Chapter 203
MSEG Service Configuration Mode Commands

The MSEG Service Configuration Mode allows you to configure Mobile Service Edge Gateway (MSEG) service parameters.

Important: This configuration mode is not supported in this release. For more information please contact your Cisco account representative.



associate

This command allows you to configure accounting policy for the MSEG service.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

associate accounting-policy *accounting_policy_name*

no associate accounting-policy

no

Deletes the specified associate accounting-policy configuration.

accounting_policy_name

Specifies the accounting policy for the current MSEG service.
accounting_policy_name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the accounting policy for an MSEG service.

Example

The following command associates the accounting policy named *test* to the current MSEG service:

```
associate accounting-policy test
```

bind gtpc-address

This command allows you to bind specific GTP-C address to the MSEG service.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

bind gtpc-address *ipv4/ipv6_address* **[udp-port** *port_number* **]**

no bind gtpc-address

no

If previously configured, deletes the bind GTP-C address configuration.

ipv4/ipv6_address

Specifies the GTP-C IP address for the service in IPv4 dotted-decimal or IPv6 colon-separated notation.

udp-port *port_number*

Specifies the UDP port number.
port_number must be an integer from 1 through 65535.

Usage

Use this command to configure the GTP-C IP address for an MSEG service.

Example

The following command configures the GTP-C address *1.1.1.1* and the UDP port *111* in the current MSEG service:

```
bind gtpc-address 1.1.1.1 udp-port 111
```

bind gtpu-address

This command allows you to bind specific GTP-U address to the MSEG service.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

[no] bind gtpu-address *ipv4/ipv6_address*

no

Deletes the specified bind GTP-U address configuration.

ipv4/ipv6_address

Specifies the GTP-U IP address for the service in IPv4 dotted-decimal or IPv6 colon-separated notation.
Up to four GTP-U addresses can be configured for each MSEG service instance.

Usage

Use this command to configure the GTP-U IP address for the current MSEG service.
Up to four GTPU addresses can be configured for each MSEG service instance.

Example

The following command configures the GTP-U address *1.1.1.1* for the current MSEG service:

```
bind gtpu-address 1.1.1.1
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

gtpc

This command allows you to configure GTP-C transmission-related parameters.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

gtpc { echo-interval *echo_interval* **| max-retransmissions** *max_retransmissions* **| retransmission-timeout** *retransmission_timeout* **}**

{ default | no } gtpc { echo-interval | max-retransmissions | retransmission-timeout }

default

Configures the default setting for the specified parameter.

- **echo-interval**: 60 seconds
- **max-retransmissions**: 4
- **retransmission-timeout**: 5 seconds

no

Deletes the configuration for the specified parameter.

echo-interval *echo_interval*

Specifies the echo interval (in seconds).
echo_interval must be an integer from 60 through 3600.
Default: 60

max-retransmissions *max_retransmissions*

Specifies the maximum number of retries for GTP Control packets.
max_retransmissions must be an integer from 0 through 15.
Default: 4

retransmission-timeout *retransmission_timeout*

Specifies the control packet retransmission timeout duration in GTP (in seconds).
retransmission_timeout must be an integer from 1 through 20.
Default: 5

Usage

Use this command to configure GTP-C transmission related parameters.

Example

The following command configures the GTP-C retransmission-timeout parameter to *11* seconds:

```
gtpc retransmission-timeout 11
```

gtpu

This command allows you to configure GTP-U transmission-related parameters.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

gtpu { echo-interval *echo_interval* **| max-retransmissions** *max_retransmissions* **| retransmission-timeout** *retransmission_timeout* **}**

{ default | no } gtpu { echo-interval | max-retransmissions | retransmission-timeout }

default

Configures the default setting for the specified parameter.

- **echo-interval**: Disabled
- **max-retransmissions**: 4
- **retransmission-timeout**: 5 seconds

no

Deletes the configuration for the specified parameter.

echo-interval *echo_interval*

Specifies the echo interval (in seconds) for MSEG.
echo_interval must be an integer from 60 through 3600.
Default: Disabled

max-retransmissions *max_retransmissions*

Specifies the maximum number of retries for GTP-U packets.
max_retransmissions must be an integer from 0 through 15.
Default: 4

retransmission-timeout *retransmission_timeout*

Specifies the control packet retransmission timeout duration (in seconds) in GTP.
retransmission_timeout must be an integer from 1 through 20.
Default: 5

Usage

Use this command to configure GTP-U transmission related parameters.

Example

The following command configures the GTP-U retransmission-timeout parameter to *11* seconds:

```
gtpu retransmission-timeout 11
```

mseg-criteria

This command allows you to configure MSEG criteria for the MSEG service instance.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

mseg-criteria *mseg_criteria_name*

no mseg-criteria

no

Deletes the MSEG criteria configuration.

mseg_criteria_name

Specifies name of the MSEG criteria.
mseg_criteria_name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the MSEG criteria for an MSEG service instance.

Important: If an MSEG criteria is not configured for the MSEG service instance, the service will default to forwarding the calls to the respective GGSNs.

For information on configuring offload criteria, see the *MSEG Offload Criteria Configuration Mode Commands* chapter.

Example

The following command configures the MSEG criteria named *test* for the current MSEG service:

```
mseg-criteria test
```

mseg-id

This command allows you to configure the identifier for the MSEG instance represented by the MSEG service instance.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

mseg-id *mseg_id*

no mseg-id

no

Deletes the MSEG ID configuration for the current MSEG service.

mseg_id

Specifies the MSEG ID.
mseg_id must be an integer from 1 through 65535.

Usage

Use this command to configure the identifier for the MSEG instance represented by the MSEG service.

Example

The following command configures the MSEG ID *111* for the current MSEG service:

```
mseg-id 111
```

path-failure

This command allows you to configure the policy to be used for path failure detection.

Important: This command is not supported in this release. For more information please contact your Cisco account representative.

Product

MSEG

Privilege

Security Administrator, Administrator

Syntax

```
path-failure detection-policy gtp { echo | non-echo + }

{ default | no } path-failure detection-policy
```

default

Configures the default setting – gtpc/gtpu echo message. Path failure is detected on echo.

no

Deletes the path-failure detection-policy configuration.

echo

Specifies echo. Path failure is detected when the retries of echo messages are exceeded.

non-echo

Specifies other than echo. Path failure is detected when the retries of non-echo messages are exceeded.

+

Indicates that more than one of the keywords can be entered in a single command.

Usage

This command configures path failure detection policy.

Example

The following command configures the path failure detection policy to non-echo:

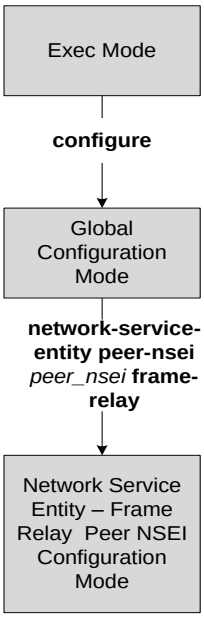
```
path-failure detection-policy gtp non-echo
```

Chapter 204
Network Service Entity - Peer NSEI Configuration Mode Commands

The Network Service Entity (NSE) - Peer NSEI configuration mode configures the Frame Relay parameters for the peer NSE. This mode is a sub-mode of the Global Configuration mode. This sub-mode provides the commands and parameters to define the management functionality for the Gb interface between a BSS and an SGSN over a 2.5G GPRS Frame Relay network connection.

Upon accessing this mode, the prompt should be similar to:

```
[local]hostname(nse-fr-peer-nsei-<nse_id>)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

bssgp-timer

This command has been deprecated.

end

Exits the current configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Return to the Exec mode.

exit

Exits the current configuration mode and returns to the previous configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the global configuration mode.

ns-reset-mode

The command configures automatic NS-Reset for a specific Frame Relay peer NSE (network service entity).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
ns-reset-mode { active | passive }

default ns-reset-mode
```

default

Resets the configuration to the passive mode.

active

Configures active mode so that the SGSN is enabled to initiate NS-Reset without manual intervention.

passive

Configures passive mode which means the SGSN continues *not* to initiate NS-Reset.
This is the default mode.

Usage

Use this command to configure the SGSN for active mode regarding the peer NSE, so that the SGSN will initiate:

- NS-Reset when NSVC-DLCI binding is done.
- NS-Reset when the link goes down and then comes back.
- NS-Unblock upon receipt of NS-Reset-Ack message.

Active mode is useful in the following scenarios:

- if the SGSN detects LMI down but the BSC does not detect any link failure so does not send NS-Reset.
- if the NS layer can go down and the SGSN will mark the link as 'Blocked-Dead'. If the link comes up later, the NS layer state for that link will remain in the Blocked state.

Example

Configure active mode to perform NS-Reset when the link goes down and comes back up:

```
ns-reset-mode active
```

ns-vc

This command creates a network service virtual circuit (NSVC) for this frame relay NSE and enters the configuration sub-mode to define the NSVC parameters. These parameters are described in the NSVC Configuration Mode chapter elsewhere in this CLI Reference Guide.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] ns-vc id *ns-vc_id*

no

Removes the specified NSVC configuration.

id *ns-vc_id*

This keyword defines the NSVC configuration identifier.
ns-vc_id: Must be an integer from 0 to 65535

Usage

Access the NSVC configuration mode.

Example

Gain access to the NSVC configuration mode to change the 4th instance.

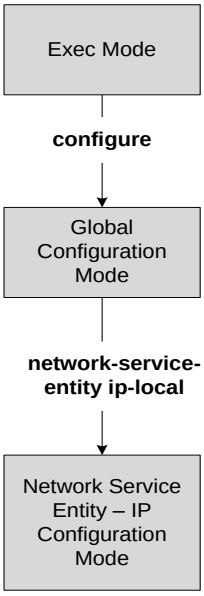
```
ns-vc id 4
```

Chapter 205
Network Service Entity- IP Local Configuration Mode Commands

The Network Service Entity (NSE) - IP Local configuration mode is a sub-mode of the Global Configuration mode. This sub-mode configures the local endpoint for NS/IP with the commands and parameters to define the management functionality for the Gb interface between a BSS and an SGSN over a 2.5G GPRS IP network connection.

Upon entering this mode, the prompt will appear in a manner similar to:

```
[local]hostname(nse-ip-local)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

all-nsvc-failure-action

Configure how the SGSN handles the NSE when all NSVCs go down.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
all-nsvc-failure-action clear-nse

default all-nsvc-failure-action
```

default

By default, the NSE is not cleared if all NSVCs go down.

clear-nse

Instructs the SGSN to SGSN to clear NSEs if all NSVCs to the BSC are down.

Usage

Enable the SGSN to clear NSE information when all NSVCs go down.

Example

Use the following command to configure the SGSN to clear NSEs when all NSVCs go down.

```
all-nsvc-failure-action clear-nse
```

bssgp-timer

This command has been deprecated.

end

Exits the current configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Return to the Exec mode.

exit

Exits the current configuration mode and returns to the global configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Returns to the global configuration mode.

max-ns-retransmissions

This command configures the maximum number of transmission retries counter.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[default] max-ns-retransmissions { alive *count* **| sns-proc** *count* **}**

default

Resets the specified counter configuration to the default value.

alive *count*

Sets the maximum number of alive retries.
count: Must be an integer between 0 and 10. Default is 3.

sns-proc *count*

Sets the maximum number of retries for the SNS procedure
count: Must be an integer between 0 and 5. Default is 3.

Usage

Sets the maximum for NS transmission retries.

Example

```
max-ns-retransmission alive 4
```

ns-timer

This command sets the network service (NS) counters for the SNS procedure and testing.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ns-timer { sns-prov *timeout_val* **| test** *timeout_val* **}**

default ns-timer { sns-prov | test }

default

Resets the selected timer configuration to its default value.

sns-prov *timeout_val*

Sets the SNS procedure timeout value in seconds.
timeout_val: Enter an integer from 1 to 10. Default is 5.

test *timeout_val*

Sets the test procedure timeout value in seconds.
timeout_val: Enter an integer from 1 to 60. Default is 30 seconds.

Usage

Set NS timers to help manage the NSE-IP connection.

Example

The following example sets the test timer to 4 seconds:

```
ns-timer test 4
```

nsvc-failure-action

This command enables and disables the sending of an NS-STATUS message with cause ‘ip-test fail’ when NSVC goes down.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

nsvc-failure-action send-ns-status

default nsvc-failure-action

default

Resets the command configuration to its default value. The default action is not to send an NS-STATUS message. This is applicable only to NSVCs that are auto-learned and not configured.

send-ns-status

Enables the sending of the NS-STATUS message.

Usage

Use this command to enable or disable sending an NS-STATUS messages when an NSVC goes down.

Example

Enable sending of the message:

```
nsvc-failure-action send-ns-status
```

nsvl

This command creates and instance of a network service virtual link (NSVL) and enters the NSVL configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] nsvl instance *nsvl_id*

no

Removes the identified NSVL definition from the configuration.

instance *nsvl_id*

Identifies a specific NSVL configuration instance.
nsvl_id: Must be an integer from 0 to 3.

Usage

Access the NSVL configuration mode.

Example

Enter the NSVL configuration sub-mode to modify the configuration for NSVL instance 2:

```
nsvl instance 2
```

peer-network-service-entity

This command has been replaced by the Network Service Entity - Peer NSEI Frame Relay configuration mode.

retry-count

This command has been replaced by the **max-ns-retransmissions** command.

timer

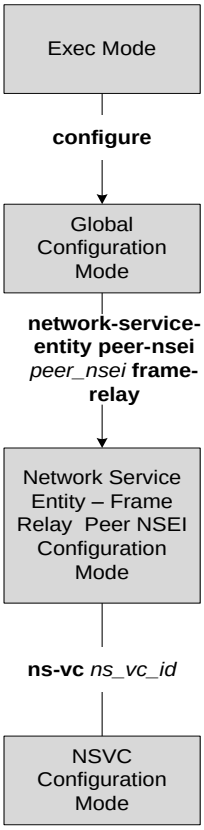
This command has been replaced by the **ns-timer** command.

Chapter 206
Network Service Virtual Connection Configuration Mode Commands

The Network Service Virtual Connection (NSVC) configuration mode is a sub-mode of the Network Service Entity (NSE) - Peer NSEI (for Frame Relay) configuration mode. The NSVC sub-mode creates a configuration instance for a specific NSVC, within the Gb interface, between a BSS and an SGSN in a 2.5G GPRSFrame Relay network connection.

Upon accessing this mode, the prompt will appear similar to:

```
[local]hostname(nse-fr-peer-nsei-<nse_id>-nsvci-<nsvc_id>)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Return to the Exec mode.

exit

Exits the current configuration mode and returns to the previous configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

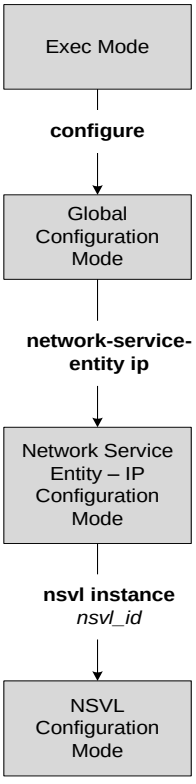
Returns to the network service entity - frame relay configuration mode.

Chapter 207
Network Service Virtual Link Configuration Mode Commands

The Network Service Virtual Link configuration mode is a sub-mode of the Network Service Entity - IP configuration mode. This sub-mode provides the commands and parameters to define the NSVL of the Gb interface between a BSS and an SGSN in a 2.5G GPRS IP network connection.

Upon entering this mode, the prompt should appear similarly to the following:

```
[local]hostname(nse-ip-local-nsvl-<nsvl_id>)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Return to the Exec mode.

exit

Exits the current configuration mode and returns to the previous configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Return to the network service entity - IP configuration mode. mode.

nsvl-address

This command configures the IP address of the NSVL. end-point.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

nsvl-address ip-address *ip_address* **context** *ctxt_name* **port** *port_num*

ip-address *ip_address*

Identifies the address of the NSVL.
ip_address: Must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6.

context *ctxt_name*

Identifies the specific context associated with this NSVL address.
ctxt_name: Enter up to 79 alphanumeric characters.

port *port_num*

Specifies the UDP port to associate with the NSVL end-point.
port_num: Must be an integer from 1 to 65535.

Usage

Use this command to configure the IP address, context name and port number for the NSVL end-point.

Example

nsvl-address ip-address *1.1.1.1* **context** *sgsn2* **port** *3735*

weight

This command configures the signaling or data weight for NSVL.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

weight { data *data_weight* **| signaling** *signaling_weight* **}**

data *data_weight*

Defines the data weight for the NSVL.
data_weight: Must be an integer from 0 to 255. Default is 1.

signaling *signaling_weight*

Defines the signaling weight for the NSVL.
signaling_weight: Must be an integer from 0 to 255. Default is 1.

Usage

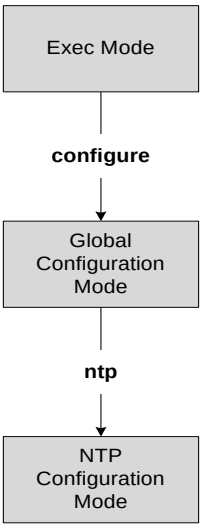
Configure the weight of the signaling or data for the NSVL.

Example

weight data *234*

Chapter 208
NTP Configuration Mode Commands

The NTP Configuration Mode is used to manage the Network Timing Protocol (NTP) options for the entire system.



enable

Enables the use of the network timing protocol for updating the system clock.

Product

All

Privilege

Security Administrator, Administrator

Syntax

enable [*context* **]**

context

Default: local
Specifies the context for which NTP is to be enabled. *name* must refer to a previously configured context expressed as an alphanumeric string of 1 through 79 characters.

Usage

Sets the NTP server to be used for the system. Only one NTP server may be active at any given time. If this command were issued in a different context followed by the current context, the prior context's NTP server would be disabled and the current context's NTP server would be used.
If any NTP server is enabled, the chassis system clock will be synchronized to the active NTP server which covers all contexts for timing synchronization.
The use of a given context for NTP server assignment allows the server to inherit the domain and IP routing options of that context.

Example

```
enable NTPcontext
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

server

Configures an NTP server for use by the local NTP client in synchronizing the system clock.

Product

All

Privilege

Security Administrator, Administrator

Syntax

server *ip_address* **[prefer] [version** *number* **] [minpoll** *poll_period* **] [maxpoll** *poll_period* **]**

no server *ip_address*

no

Indicates the server specified is to be removed from the list of NTP servers for clock synchronization.

ip_address

Specifies the IP address of the NTP server to allow for clock synchronization. *ip_address* must be specified using the IPv4 dotted-decimal notation.

prefer

Indicates the NTP server specified to be the preferred server. Only one server can be set to preferred. The preferred server is the first one contacted for clock synchronization.

Important: Use of the **prefer** keyword is not recommended.

version *number*

Default: 4
Specifies the network timing protocol version to use for server communications. *number* must be an integer from 1 to 4.

minpoll *poll_period*

Default:6
Specifies the minimum polling interval (in seconds) for NTP messages as a power of 2. *poll_period* is the power or exponent. For example, if you specify the number 10, the value is 2^10 and the resultant poll period is 1024 seconds. *poll_period* must be an integer from 6 through 17.

maxpoll *poll_period*

Default: 10
Specifies the maximum polling interval (in seconds) for NTP messages as a power of 2. *poll_period* is the power or exponent. For example, if you specify the number 10, the value is 2^10 and the resultant poll period is 1024 seconds. *poll_period* must be an integer from 6 through 17.

Usage

Configure the network timing protocol servers in the network as changes occur.

Important: Adding, removing, or modifying an NTP server configuration entry causes the NTP client to restart and restart the synchronization process with all configured NTP servers.

Example

The following command adds the NTP server with address *10.2.3.4* to the list of NTP servers.

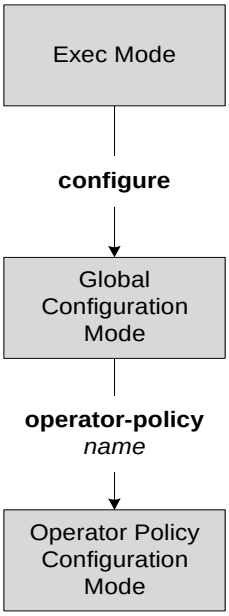
```
server 10.2.3.4
```

Chapter 209
Operator Policy Configuration Mode

Operator Policy configuration mode associates APNs, APN profiles, IMEI ranges, IMEI profiles, an APN remap table and a call control profile to an operator policy. These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies.

- A maximum of 1,000 operator policies can be defined, including the "default" operator policy.
- A maximum of 128 APN profiles can be associated with a single operator policy.
- A maximum of 128 IMEI profiles can be associated with a single operator policy.
- Only one APN remap table can be associated with a single operator policy.
- Only one call control profile can be associated with a single operator policy.

Using the Operator Policy feature allows the operator to fine-tune any desired restrictions or limitations needed to control call handling per subscriber or for a group of callers across IMSI ranges.



apn

This command identifies an APN (access point name) and associates it with an APN profile (created separately in the APN Profile Configuration mode).

Product

MME, S-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

apn { default-apn-profile *apn_profile_name* **| network-identifier** *apn_net_id* **apn-profile** *apn_profile_name* **| operator-identifier** *apn_op_id* **apn-profile** *apn_profile_name* **}**

no apn { default-apn-profile | network-identifier *apn_net_id* **| operator-identifier** *apn_op_id* **}**

no

Disables the specified APN to APN Profile correspondence.

default-apn-profile *apn_profile_name*

Enables the use of a default APN profile comprised of default values for all parameters. this profile will be used when none of the configured APNs match the APN in the incoming Request.
apn_profile_name must be an alphanumeric string of 1 through 64 characters.

apn-profile*apn_profile_name*

apn_profile_name must be an alphanumeric string of 1 through 64 characters.

network-identifier *apn_net_id*

Links the specified APN network ID with the specified APN profile.
apn_net_id must be an alphanumeric string of 1 through 63 characters, including dots (.) and dashes (-).

operator-identifier *apn_op_id*

Links the specified APN operator ID with the specified APN profile.
apn_op_id: must be an alphanumeric string of 1 through 18 characters, including dots (.). The string must be in the following format, where # represents a digit: MNC###.MCC###.GPRS.

Usage

Use this command, to associate APNs with APN profiles. This command can be repeated to associate multiple APNs with profiles.

Example

Associate the APN profile named *apnprof1* to APN network ID *starflash.com*:

```
apn apnprof1 network-identifier starflash.com
```

associate

Associate an APN remap table and a call control profile with the operator policy.

Product

MME, S-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

associate { apn-remap-table *table_id* **| call-control-profile** *profile_id* **}**

no associate { apn-remap-table | call-control-profile }

no

Removes the association definition from the policy configuration.

apn-remap-table *table_id*

Identifies the APN remap table to be associated with the operator policy.
table_id must be an alphanumeric string of 1 through 65 characters.

call-control-profile *profile_id*

Identifies a call control profile to be associated with the operator policy.
profile_id must be an alphanumeric string of 1 through 64 characters.

Usage

Use this command to associate an APN remap table and/or a call control profile with this Operator Policy. The APN remap table and the call control profile contain the definitions that instruct the SGSN or MME how to handle calls. Only one of each of these can be associated with an operator policy.

Example

Associate the *stardust.net_APNremap1* APN remap table with this operator policy:

```
associate apn-remap-table stardust.net_APNremap1
```

description

Associates a description with or names an operator policy.

Product

MME, S-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

description *description*

no description

description

Enter an alphanumeric string of 1 through 100 characters. If the string includes spaces, punctuation, and case-sensitive letters, it must be bracketed with double quotation marks (“ “).

no

Removes the existing description from this operator policy.

Usage

Identity this particularly operator policy using descriptive text.

Example

```
description “sgsn1 operator policy carrier1”
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

imei

Defines a range of IMEI (International Mobile Equipment Identity) numbers and associates an IMEI profile with the range definition.

Product

MME, S-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

imei range *IMEI_number* **to** *IMEI_number* **{ imei-profile** *profile_name* **| sv** *##* **imei-profile** *profile_name* **}**

no imei range *IMEI_number* **to** *IMEI_number* **sv** *##*

no

Removes the IMEI definition from the policy configuration.

range *IMEI_number* **to** *IMEI_number*

Defines the beginning and end of a range of IMEIs.
IMEI_number must be a numerical string of up to 14 digits.

sv *##*

Identifies the software version to fine-tune the IMEI definition. This keyword should only be included if the IMEISV is retrievable.
must be a 2-digit integer.

imei-profile *profile_name*

Identify the IMEI profile that defines the actions appropriate to the devices identified within the specified range.
profile_name must be an alphanumeric string of 1 through 64 characters.

Usage

This command defines the IMEI ranges that will be used by the operator policy to determine if the device is appropriately selected for actions defined in the specified IMEI profile.

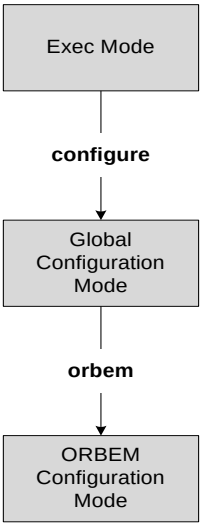
Example

All devices with an IMEI of *123123** requesting Attach shall be subject to actions in the *blacklist_profile1*

```
imei range 1231230 to 1231239 imei-profile name blacklist_profile1
```

Chapter 210
ORBEM Configuration Mode Commands

The ORBEM Configuration Mode is used to manage the Object Request Broker Element Manager (ORBEM) server options for the current context.



activate

Activates/deactivates a Common Object Request Broker Architecture (CORBA) client for the ORBEM interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

active client *id*

no active client *id*

no

Indicates the client specified is to be deactivated. When omitted, the client is activated.

id *name*

Specifies the client to be activated. *name* must refer to a previously configured client expressed as an alphanumeric string of 1 through 10 characters.

Usage

Activates CORBA clients after they have been configured or deactivated by the system or by configuration.

Example

```
active client wem

no active client wem
```

client

Configures/removes a CORBA client from the ORB element manager system interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

client id *name* **[encrypted] password** *pwd*

no client id *name*

no

Indicates the client specified is to be removed from the configuration.

id *name*

Specifies the client to be configured. *name* must be an alphanumeric string of 1 through 10 characters.

encrypted

Indicates password specified is encrypted.
The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

password *pwd*

Specifies the password for the CORBA client. *pwd* must be an alphanumeric string of 1 through 35 characters.

Usage

ORBEM clients must be configured prior to being activated.

Example

The following commands set the password for client *wem* specifying a plain text password and an encrypted password as well.

```
client id wem password wem1001

client id wem encrypted password f54gj801sd
```

The following deletes *wem* from the configuration.

```
no client id wem
```

default

Restores the system default values for the option specified.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
default { event-notif-iiop-port | event-notif-service filter | event-notif-siop-port |
iiop-port | iop-address | max-attempt | session-timeout | siop-port }
```

event-notif-iiop-port

Restores the port number for the inter-ORB event notifications to the system default: 7778.

event-notif-service filter

Restores the ORB Notification Service filter to its default behavior of sending all “error” level and higher events, and “info” level events for the orbs facility, CLI command logs, and license change logs.

event-notif-siop-port

Restores the port to use for secure socket layer inter-ORB event communication to the system default: 7777.

iiop-port

Restores the port number for inter-ORB communications to the system default: 14132.

iop-address

Restores the IP address for inter-ORB communications to the system default: IP address of current context.

max-attempt

Restores the maximum number of failed login attempts before which the client is deactivated to the system default: 3 attempts.

session-timeout

restores the amount of idle time (no activity) before a session is terminated to the system default: 300 seconds.

siop-port

Restores the secure socket layer I/O port for inter-ORB events to the system default: 14131.

Usage

Restore the ORB element manager options to a well known values, the system defaults.

Example

```
default event-notif-iiop-port
```

default max-attempt

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

event-notif-iiop-port

Configures the port number for Internet inter-ORB event notifications.

Product

All

Privilege

Security Administrator, Administrator

Syntax

event-notif-iiop-port *number*

number

Default: 7778
Specifies the port number to use as an integer from 1 through 65535.

Usage

Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for standardized inter-ORB communications.
Event notification port configured is only used if the Internet inter-ORB transport is enabled via the **iiop-transport** command with the event notification service being enabled as well.

Example

```
event-notif-iiop-port 25466
```

event-notif-service

Enables or disables the ORB Notification Service and allows the configuration of filters dictating which event notifications are sent.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] event-notif-service [filter { event-id *event_id* **[to** *final_event_id* **] | facility** *event_facility* **level** *event_level* **}]**

---

no

Disables the event notification service.

---

filter

Specifies a filter that determines for which events the system sends notifications.

---

event-id *event_id* **[to** *final_event_id* **]**

Specifies an event filter based on event identification (event ID) number.
event_id is a specific event ID to filter or is the initial event ID in range if the **to** keyword is used. It can be configured to an integer from 1 through 100000.
to allows the specification of a range of event IDs to filter. When used, *final_event_id* specifies the last event ID in the range to be filtered. It can be configured to an integer from 1 through 100000, but must be a value greater than the initial event ID.

---

facility *event_facility* **level** *event_level*

Specifies an event filter based on facility type and notification severity level.
event_facility specifies the facility type and can be any one of the following:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: AAA client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **aal2**: AAL2 protocol logging facility
- **acl-log**: Access Control List logging facility
- **acsctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: Active Charging Service (ACS) Manager facility
- **alarmctrl**: Alarm Controller facility
- **alcap**: ALCAP protocol logging facility

- **alcapmgr**: ALCAPMgr logging facility
- **all**: All facilities
- **asngwmgr**: ASN Gateway Manager facility
- **asnpcmgr**: ASN Paging Controller Manager facility
- **bfd**: BFD protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux Manager
- **bngmgr**: BNG demuxmgr logging facility
- **bssap+**: Bssap+ logging facility
- **bssgp**: BSSGP Protocol logging facility
- **callhome**: CALLHOME application logging facility
- **cap**: CAP Protocol logging facility
- **cli**: CLI logging facility
- **connproxy**: Connection Proxy logging facility
- **credit-control**: Credit Control facility
- **cscf**: IMS/MMD CSCF
- **cscfmgr**: SIP CSCF Manager facility
- **cscfrtcp**: CSCF RTCP protocol logging facility
- **cscfrtp**: CSCF RTP protocol logging facility
- **cscfttmgr**: SIP CSCFTT Manager facility
- **csp**: Card Slot Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: Content Service Selection (CSS) RADIUS Signaling facility
- **cx-diameter**: Cx Diameter messages
- **dcardctrl**: IPSec Daughter Card Controller logging facility (not used at this time)
- **dcardmgr**: IPSec Daughter Card Manager logging facility (Not used at this time)
- **demuxmgr**: Demux Manager API facility
- **dgmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: DHCP facility (GGSN product only)
- **dhcpv6**: DHCPV6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting
- **diameter-auth**: Diameter Authentication
- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ECS Diameter signaling facility

- **diameter-hdd**: Diameter HDD Interface
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSec Data Path facility
- **drvctrl**: Driver Controller facility
- **eap-diameter**: EAP Diameter messages
- **eap-ipsec**: EAP
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface Logging facility
- **egtpc**: EGTP Control plane
- **egtpmgr**: EGTP Demux manager
- **egtpu**: EGTP User plane
- **epdg**: EPDG logging facility
- **event-notif**: Event Notification Interface logging facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
- **fng**: FNG logging facility
- **gmm**: GMM Protocol logging facility
- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS-NS Protocol logging facility
- **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages
- **gss-gcdr**: GTPP Storage Server GCDR facility
- **gtpc**: GTP-C protocol logging facility (GGSN product only)
- **gtpcmgr**: GTP-C protocol Manager logging facility (GGSN product only)
- **gtpp**: GTP-PRIME protocol logging facility (GGSN product only)
- **gtpu**: GTP-U protocol logging facility (GGSN product only)
- **gtpumgr**: GTPU Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages
- **gy-diameter**: Gy Diameter messages
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **hdctrl**: HD Controller logging facility
- **hnb-gw**: HNB-GW (3G Femto GW) logging facility
- **hnbmgr**: HNBMGR (3G Femto GW DemuxMgr) logging facility
- **hss-peer-service**: HSS Peer Service facility
- **igmp**: IGMP
- **ikev2**: IKEv2

- **ims-authorizatn**: IMS Authorization Service facility
- **ims-sh**: HSS SH Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **imsue**: IMSUE
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipms**: IPMS logging facility
- **ipsec**: IP Security logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ipsp**: IP Pool Sharing Protocol logging facility
- **kvstore**: KV Store facility
- **l2tp-control**: L2TP control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: LAGMGR logging facility
- **ldap**: LDAP Messages
- **li**: Refer to the *Lawful Intercept Configuration Guide* for a description of this command.
- **linkmgr**: SGSN/SS7 Links Manager facility
- **llc**: LLC Protocol logging facility
- **local-policy**: Local Policy Service facility
- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway logging facility
- **map**: MAP Protocol logging facility
- **megadiameter**: Megadiameter Manager (SLF Service)
- **mme-app**: MME application facility
- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: MME Demux Manager facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 control logging facility
- **mseg-app**: MSEG application logging facility
- **mseg-gtpc**: MSEG GTPC application logging facility

- **mseg-gtpu**: MSEG GTPU application logging facility
- **msegmgr**: MSEG demuxmgr logging facility
- **mtp2**: MTP2 Service logging facility
- **mtp3**: MTP3 Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **npuctrl**: Network Processor Unit Control facility
- **npumgr**: Network Processor Unit Manager facility
- **npumgr-acl**: NPUMGR ACL logging facility
- **npumgr-drv**: NPUMGR DRV logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility
- **npumgr-fwd**: NPUMGR FWD logging facility
- **npumgr-init**: NPUMGR INIT logging facility
- **npumgr-lc**: NPUMGR LC logging facility
- **npumgr-port**: NPUMGR PORT logging facility
- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **npumgr-vpn**: NPUMGR VPN logging facility
- **npusim**: NPUSIM logging facility
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF logging facility
- **ospfv3**: OSPFv3 protocol logging facility
- **p2p**: Peer-to-Peer detection logging facility
- **pccmgr**: IPCF PCC Manager library
- **pdg**: PDG logging facility
- **pdgmgr**: PDG Manager facility
- **pdif**: PDIF logging facility
- **pgw**: PDN Gateway facility
- **phs**: Payload Header Suppression
- **phs-control**: PHS X1/X5 and X2/X6 Interface logging facility
- **phs-data**: PHS Data logging facility
- **phs-eapol**: PHS EAPOL logging facility
- **phsgwmgr**: PHS Gateway Manager facility
- **phspcmgr**: PHS Paging Controller Manager facility
- **pmm-app**: PMM application logging facility
- **ppp**: PPP link and packet facilities
- **pppoe**: PPPOE logging facility
- **push**: VPNMGR CDR push logging facility
- **radius-acct**: RADIUS accounting logging facility

- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: RANAP Protocol logging facility
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Rf Diameter messages
- **rip**: RIP logging facility (RIP is not supported at this time.)
- **rohc**: RObust Header Compression facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RUA (3G Femto GW - RUA messages) logging facility
- **s1ap**: S1AP Protocol logging facility
- **sccp**: SCCP Protocol logging facility
- **sct**: Shared Configuration Task logging facility
- **sctp**: SCTP Protocol logging facility
- **sess-gr**: SM GR facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs protocol logging facility
- **sgsn-app**: SGSN-APP interface logging facility
- **sgsn-failures**: SGSN call failures logging facility
- **sgsn-gtpc**: SGSNs GTP-C Protocol logging facility
- **sgsn-gtpu**: SGSNs GTP-U Protocol logging facility
- **sgsn-mbms-bearer**: SGSNs MBMS bearer app (SMGR) logging facility
- **sgsn-misc**: SGSN miscellaneous logging facility
- **sgsn-system**: SGSNs System Components logging facility
- **sgsn-test**: SGSN Tests logging facility
- **sgtpmgr**: SGSN GTPC Manager facility
- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages
- **sitmain**: System Initialization Task main logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: SMS Service logging facility
- **sndcp**: SNDCP Protocol logging facility
- **snmp**: SNMP logging facility

- **sprmgr**: IPCF SPR Manager library
- **srdb**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **ssh-ipsec**: SSH IP Security logging facility **stat:** Statistics logging facility
- **ssl**: SSL (Secure socket layer messages) logging facility
- **stat**: Statistics logging facility
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **tcap**: TCAP Protocol logging facility
- **threshold**: Threshold logging facility
- **ttg**: TTG logging facility
- **tucl**: TUCL logging facility
- **udr**: Usage Detail Record facility (used with the Charging Service)
- **user-data**: User data logging facility
- **user-l3tunnel**: User layer-3 tunnel logging facility
- **usertcp-stack**: User Tcp Stack
- **vpn**: Virtual Private Network logging facility
- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6

event_level

specifies the severity level of the event notification to filter and can be configured to one of the following:

- critical: display critical events
- error: display error events and all events with a higher severity level
- warning: display warning events and all events with a higher severity level
- unusual: display unusual events and all events with a higher severity level
- info: display info events and all events with a higher severity level
- trace: display trace events and all events with a higher severity level
- debug: display all events

Usage

This command is used to enable or disable the ORB Notification Service. Additionally, it can be used to configure filters dictating which events are sent. This service is disabled by default.
Filters can be configured for a specific event identification number (event ID), a range of event IDs, or specific severity levels for events for particular facilities.
When no filters are configured and the service is enabled, the ORB Notification Service sends all “error” level and higher events, and “info” level events for the orbs facility, CLI command logs, and license change logs.
Multiple instance of this command can be executed to configure multiple filters.

Example

The following command enables the ORB Notification service:

```
event-notif-service
```

The following command disables the ORB Notification service:

```
no event-notif-service
```

The following command configures a filter for the ORB Notification Service allowing only event IDs *800* through *805* to be sent:

```
event-notif-service filter event-id 800 to 805
```

The following command configures a filter for the ORB Notification Service allowing only *critical* level notifications for all facilities:

```
event-notif-service filter facility all level critical
```

event-notif-siop-port

Configures the port to use for secure socket layer (SSL) inter-ORB event communication.

Product

All

Privilege

Security Administrator, Administrator

Syntax

event-notif-siop-port *number*

number

Default: 7777
Specifies the port number to use as an integer from 1 through 65535.

Usage

Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for inter-ORB communications using SSL.

Example

```
event-notif-siop-port 25466
```

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

iiop-port

Configures the port number for Internet Inter-ORB Protocol (IIOP) communications.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] iiop-port *number*

no

Disables the IIOP port.

number

Default: 14132
Specifies the port number to use as an integer from 1 through 65535.

Usage

Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for standardized inter-ORB communications.
Internet inter-ORB port is only used if IIOP transport is enabled via the **iiop-transport** command.

Example

```
iiop-port 25466
```

iiop-transport

Enables/disables use of the Internet Inter-ORB Protocol (IIOP) for management across the network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
iiop-transport

no iiop-transport
```

no

Disables internet inter-ORB protocol communication across the network.

Usage

Enables the transport of IIOP messages to support remote management across the network.
The default is IIOP transport disabled.

Example

The following commands enable and disable the ORB-based management across the network, respectively.

```
iiop-transport

no iiop-transport
```

iop-address

Sets the IP address used by the ORBEM Server to advertise service.

Product

All

Privilege

Security Administrator, Administrator

Syntax

iop-address *ip_address*

ip_address

Specifies the IP address to use for inter-ORB communications for the current context. *ip_address* must be specified using IPv4 dotted-decimal notation.

Usage

Change the inter-ORB IP address when the IP address of the current context should not be used. The IP address of the local context may not be appropriate when the ORB configuration across nodes would cause conflicts with the IP addresses.
The default inter-ORB IP address is the IP address of the current context.

Example

```
iop-address 10.2.3.4
```

max-attempt

Configures the maximum number of failed login attempts after which the client is deactivated.

Product

All

Privilege

Security Administrator, Administrator

Syntax

max-attempt *count*

count

Default: 3 attempts
Specifies the number of failed login attempts prior to deactivating a client. The value must be an integer from 1 through 10.

Usage

Adjust the maximum number of attempts to a smaller value to increase the security level of the system.

Example

```
max-attempt 3
```

session-timeout

Configures the amount of idle time (no activity) before a client session is terminated.

Product

All

Privilege

Security Administrator, Administrator

Syntax

session-timeout *seconds*

seconds

Default: 300 seconds
Specifies the number of seconds of idle time before a client session is terminated. The value must be must be an integer from 1 through 86400.

Usage

Reduce the session timeout when the maximum number of sessions allowed is frequently being reached. Setting this to a lower value will help release idle sessions faster to allow use by other clients.

Example

```
session-timeout 1800
```

siop-port

Configures the SSL I/O port for inter-ORB events.

Product

All

Privilege

Security Administrator, Administrator

Syntax

siop-port *number*

number

Default: 14131
Specifies the port number to use as an integer from 1 through 65535.

Usage

Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for inter-ORB communications.

Example

```
siop-port 25466
```

ssl-auth-policy

Configures the SSL peer authentication policy used by the ORBEM server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
ssl-auth-policy { auth-none | auth-once | auth-once-fail | auth-peer | auth-peer-fail }
```

auth-none | auth-once | auth-once-fail | auth-peer | auth-peer-fail

Default: **auth-none**
auth-none: ORBEM server does not authenticate the peer
auth-once: ORBEM server authenticates the peer once (no fail)
auth-once-fail: ORBEM server authenticates the peer once (fail if no certificate)
auth-peer: ORBEM server authenticates the peer every time (no fail)
auth-peer-fail: ORBEM server authenticates the peer every time (fail if no certificate)

Usage

Use to configure the peer authentication policy used by the SSL transport of ORBEM.

Example

The following command sets the policy to authenticate the peer once without failure.

```
ssl-auth-policy auth-once
```

ssl-certificate

Defines the certificate to be used by the SSL transport of ORBEM.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ssl-certificate { string *certificate* **| file** *url* **}**

string *certificate*

Specifies an ORBEM SSL certificate. *certificate* is an alphanumeric string of up to 4096 characters.

file *url*

Default: /usr/ssl/certs/orbscert.pem
Specifies an ORBEM SSL certificate file and location. *url* is an alphanumeric string of up to 1024 characters.

Usage

Use to configure the certificate to be used by the SSL transport of ORBEM. Note that if the **file** option is used, the certificate content is read from the *url* and converted into a quoted string.

Example

The following command defines the certificate *cert3.pem* file as being located in the **/usr/ssl/certs** directory:

```
ssl-certificate file /usr/ssl/certs/cert3.pem
```

The following command defines the certificate string (the string shown is abbreviated):

```
ssl-certificate string
```

"-----BEGIN CERTIFICATE-----\n\
MIIELDCCA5WgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBsTELMAkGA1UEBhMCVVMx\n\
FjAUBgNVBAgTDU1hc3NhY2h1c2V0dHMxEjAQBgNVBAcTCVRld2tzYnVyeTEeMBwG\n\
A1UEChMVU3RhcmVudCBOZXR3b3JrcyBJbmMuMSIwIAYDVQQLExlFbGVtZW50IE1h\n\
bmFnZW1lbnQgU3lzdGVtMQ4wDAYDVQQDEwVPUkJFTTEiMCAGCSqGSIb3DQEJARYT\n\
b3JiZW1AbnVsaW5raW5jLmNvbTAeFw0wMjA5MDYxMjE5MTNaFw0yMjA5MDExMjE5\n\
MTNaMIGxMQswCQYDVQQGEwJVUzEWMBQGA1UECBMNTWFzc2FjaHVzZXR0czESMBAG\n\
A1UdDgQWBBSpuGGMTwgaq8H+e70ZPIFHVZjiWDCB3gYDVR0jBIHWMIHTgBRkVBzy\n\
4zW5Gv0pXcwT07PtzCm53qGBt6SBtDCBsTELMAkGA1UEBhMCVVMxFjAUBgNVBAgT\n\
DU1hc3NhY2h1c2V0dHMxEjAQBgNVBAcTCVRld2tzYnVyeTEeMBwGA1UEChMVU3Rh\n\
cmVudCBOZXR3b3JrcyBJbmMuMSIwIAYDVQQLExlFbGVtZW50IE1hbmFnZW1lbnQg\n\

U3lzdGVtMQ4wDAYDVQQDEwVPUkJFTTEiMCAGCSqGSIb3DQEJARYTb3JiZW1AbnVs\n\
aW5raW5jLmNvbYIBADANBgkqhkiG9w0BAQQFAAOBgQATOdeDWikcoUIU8Gth9wr4\n\
Z5Fi8akXHhKhN7UMKyiW/Nn5NyfqPIA+9JwYMqwVOG8ybtfBQIGRCQodbXUm6Z9Z\n\
cM3XxWKVKHVolGS83f/JfpSLnuGkBIW8m3p/snHBH2BtgNT8OLItlTdBHedTKL72\n\
ZIxGF9/ok9hUqU4ikzQcEQ==\n\
-----END CERTIFICATE-----\n"

ssl-private-key

Configures the SSL private key used by the ORBEM server.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ssl-private-key { string *key* **| file** *url* **}**

string *key*

Specifies an ORBEM SSL private key. *key* is an alphanumeric string of up to 4096 characters.

file *url*

Default: /usr/ssl/certs/orbscert.pem
Specifies the ORBEM SSL private key file location. T*url* is an alphanumeric string of up to 1024 characters.

Usage

Use to configure the private key for the SSL transport of ORBEM. Note that if **file** option is used, the private key is read from the *url* and converted into a quoted string.

Example

The following command defines the private-key *cert3.pem* file as being located in the **/usr/ssl/certs** directory:

```
ssl-private-key file /usr/ssl/certs/cert3.pem
```

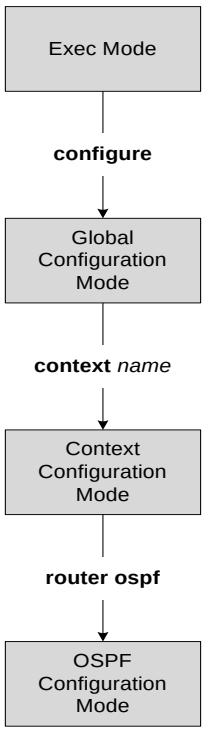
The following command defines the private-key string (the string shown is abbreviated):

```
ssl-private-key string
```

"-----BEGIN RSA PRIVATE KEY-----\n\
MIICXQIBAAKBgQC6Dh79iaK/zZG/Kwme2XS6G8/n3/+sac6huxI1WNyammyYZKZp\n\
XTjHUlS92fvn0UUM4tFjN4XoqveSiqy3IqUhnVKS3+0L7s9beanQUJuR9MdLy9Ho\n\
7qh720wpN4isqN7YfGLoqGslLQjhS8z6ZT0ZUhyusY0rE6yHTV23nHKNtQIDAQAB\n\
9br1iVWvy/N23WXwZIiH+e1tBfHqlSd/0wJBANEEOgH/vJse/YdHeYjlT76IcGRp\n\
Tq6ldBXdoLRDGUF2AqdboJ7wWCOJQO34XbBtmWFfTkqz48Mi6uh3/5kDfH8CQGAl\n\
XObwPFRztvkXprZfh7IekxAIuoHiT1JsEKSIGPzEqDY2rmoWDghOvPETO+5zWEQk\n\
TXzLaRHgbIy9MKnXSt8CQQCcBfT7VndEfG9VWyPzeL4vx4ZhUMZQ6FIJdXo7Xq9x\n\
mzX8hgIcfdg3tahlNt35gL/DjUY7d14+MgLrRf3Udbk9\n\
-----END RSA PRIVATE KEY-----\n"

Chapter 211
OSPF Configuration Mode Commands

The OSPF Configuration sub-mode is used to configure the Open Shortest Path First (OSPF) routing protocol. This mode includes commands that configure OSPF routing parameters.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

area authentication

Enables authentication for the specified OSPF area.

Product

PDSN, HA GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] area  { ipaddress | decimal_value } authentication [ message-digest ]
```

no

Disables authentication for the specified area.

ipaddress

Specifies the IP address of the area where authentication will be enabled in IPv4 dotted-decimal notation.

decimal-value

Specifies the identification number of the area where authentication will be enabled. This must be an integer from 0 through 4294967295.

authentication

Sets the OSPF authentication type to use the simple authentication method.

message-digest

Sets the OSPF authentication type to use the message digest 5 (MD5) authentication method.

Usage

Use this command to enable authentication of OPSF areas.

Example

The following command enables authentication for an OSPF area defined by the IP address *192.168.100.10* and the OSPF authentication type to MD5:

```
area 192.168.100.10 authentication message-digest
```

area default-cost

Configures the default cost for an area.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] area { ipaddress | decimal_value } default-cost cost_value
```

no

Deletes the default cost for the area.

ipaddress

Specifies the IP address of the area in IPv4 dotted-decimal notation.

decimal-value

Specifies the identification number of the area as an integer from 0 through 4294967295.

cost_value

Sets the default cost to be configured for the specified area as an integer from 0 through 16777215.

Usage

Use this command to configure the default cost for an OSPF area.

Example

The following command sets the default cost for an OSPF area defined by the IP address *192.168.100.10* to *300*:

```
area 192.168.100.10 default-cost 300
```

area nssa

Defines an area as an NSSA (Not So Stubby Area) and configures OSPF parameters for it.

Product

PDSN, HA GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] area { ipaddress | decimal_value } nssa [ default-information-originate ] [ no-redistribution ] [ no-summary ] [ translate-always ] [ translate-candidate ] [ translate-never ]
```

ipaddress

Specifies the IP address of the NSSA in IPv4 dotted-decimal notation.

decimal-value

Specifies the identification number of the NSSA area as an integer from 0 through 4294967295.

default-information-originate

Originates default information to the NSSA area.

no-redistribution

Does not redistribute external routes to the NSSA area.

no-summary

Does not inject inter-area routes into NSSA.

translate-always

Configures the NSSA-ABR (Area Border Router) to always translate

translate-candidate

Configure NSSA-ABR for translate election. (This is enabled by default.)

translate-never

Configure NSSA-ABR to never translate.

Usage

Use this command to define NSSA areas.

Example

The following command defines the area designated by the IP address *192.168.100.10* as an NSSA area:

```
area 192.168.100.10 nssa
```

area stub

Defines an area as an OSPF stub area.

Product

PDSN, HAGGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] area { ipaddress | decimal_value } stub [ no-summary ]
```

ipaddress

Specifies the IP address of the stub area in IPv4 dotted-decimal notation.

decimal-value

Specifies the identification number of the stub area as an integer from 0 through 4294967295.

no-summary

Disables (stops) the ABR (Area Border Router) from sending summary link state advertisements (LSAs) into the stub area.

Usage

Use this command to define an OPSF area as a stub area.

Example

The following command defines the OSPF area defined by the IP address *192.168.100.10* as a stub area:

```
area 192.168.100.10 stub
```

area virtual-link

Configures a virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] area { ipaddress | decimal_value } virtual-link router_id_address
```

no

Disables area virtual-link.

ipaddress

Specifies the IP address of the transit area in IPv4 dotted-decimal notation.

decimal-value

Specifies The identification number of the transit area as an integer from 0 through 4294967295.

router_id_address

Specifies the router id of the ABR to be linked to in IPv4 dotted-decimal notation.

Usage

Use this command to create a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example

The following command creates a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20*:

```
area 192.168.100.10 virtual-link 192.168.200.20
```

area virtual link authentication

Configures the OSPF authentication method to be used by the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] area { ipaddress | decimal_value } virtual-link router_id_address authentication { message-digest | null | text }
```

no

Disables area virtual link authentication.

ipaddress

Specifies the IP address of the transit ares in IPv4 dotted-decimal notation.

decimal-value

Specifies the identification number of the transit area as an integer from 0 through 4294967295.

router_id_address

Specifies the router id of the ABR to be linked to in IPv4 dotted-decimal notation.

authentication

Sets the OSPF authentication type to use the simple authentication method.

message-digest

Sets the OSPF authentication type to use the message digest (MD) authentication method.

null

Set the OSPF authentication type to use no authentication, thus disabling either MD or clear text methods.

text

Set the OSPF authentication type to use the clear text authentication method.

Usage

Use this command to set the authentication method for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example

The following command sets the authentication method for a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20* to use no authentication:

```
area 192.168.100.10 virtual-link 192.168.200.2 null
```

area virtual-link authentication-key

Configures the authentication password for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

area { *ipaddress* | *decimal_value* } **virtual-link** *router_id_address* **authentication-key** { **encrypted password** *encrypted_authentication_key* | **password** *authentication_key* }

no area { *ipaddress* | *decimal_value* } **virtual-link** *router_id_address* **authentication-key**

no

Disables the area virtual link authentication key.

ipaddress

Specifies the IP address of the transit area in IPv4 dotted-decimal notation.

decimal-value

Specifies the identification number of the transit area as an integer from 0 through 4294967295.

router_id_address

Specifies the router id of the ABR to be linked to in IPv4 dotted-decimal notation.

encrypted password

encrypted_authentication_key is an alphanumeric string of 1 through 523 characters.
Use this if you are pasting a previously encrypted authentication key into the CLI command.

password *authentication_key*

The password to use for authentication. *authentication_key* is an alphanumeric string of 1 through 16 characters that denotes the authentication password. This variable is entered in clear text format.

Usage

Use this command to specify the authentication password for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example

The following command creates an authentication password of *123456* for a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20*:

```
area 192.168.100.10 virtual-link 192.168.200.20 authentication-key password 123456
```

area virtual link intervals

Configures the interval or delay type, and the delay time in seconds, for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] area { ipaddress | decimal_value } virtual-link router_id_address [ dead-interval
value ] [ hello-interval value ] [ retransmit-interval value ] [ transmit-delay value ]
```

no

Disables the area virtual link intervals.

ipaddress

Specifies the IP address of the area in IPv4 dotted-decimal notation.

decimal-value

Specifies the identification number of the transit area as an integer from 0 through 4294967295.

router_id_address

Specifies the router id of the ABR to be linked to in IPv4 dotted-decimal notation.

dead-interval *value*

Specifies The interval (in seconds) that the router should wait, during which time no packets are received and after the router considers a neighboring router to be off-line. *value* must be an integer from 1 through 65535.

hello-interval *value*

Specifies the interval (in seconds) before sending a hello packet. *value* must be an integer from 1 through 65535.

retransmit-interval *value*

Specifies the interval (in seconds) that router should wait before retransmitting a packet. *value* must be an integer from 1 through 3600.

transmit-delay *value*

Specifies the interval (in seconds) that the router should wait before transmitting a packet. *value* must be an integer from 1 through 3600.

Usage

Use this command to set the intervals or delay types for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example

The following command sets the retransmit interval for a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20* to *60* seconds:

```
area 192.168.100.10 virtual-link 192.168.200.20 retransmit-interval 60
```

area virtual link message-digest-key

Enables the use of MD5-based OSPF authentication for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

area { *ipaddress* | *decimal_value* } **virtual-link** *router_id_address* **message-digest-key** *key_id* **md5** { **encrypted password** *encrypted_authentication_key* | **password** *authentication_key* }

no area { *ipaddress* | *decimal_value* } **virtual-link** *router_id_address* **message-digest-key** *key_id*

no

Disables the area virtual link message digest key.

ipaddress

Specifies the IP address of the transit area in IPv4 dotted-decimal notation.

decimal-value

Specifies the identification number of the transit area as an integer from 0 through 4294967295.

router_id_address

Specifies the router id of the ABR to be linked to in IPV4 dotted-decimal notation.

message-digest-key *key_id*

Specifies the key identifier number. *key_id* must be an integer from 1 through 255.

encrypted password

Specifies the use of an encrypted password. *encrypted_authentication_key* is an alphanumeric string of 1 through 523 characters.
Used this if you are pasting a previously encrypted authentication key into the CLI command.

password *authentication_key*

Specifies the password to use for authentication. *authentication_key* is an alphanumeric string from 1 through 16 characters that is entered in clear text format.

Usage

Use this command to enable the use of MD5-based OSPF authentication for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example

The following command enables the use of MD5-based OSPF authentication for a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20*, sets the MD5 Key ID to *25*, and the password to *123456*:

```
area 192.168.100.10 virtual-link 192.168.200.20 message-digest-key 25 md5 password 123456
```

capability graceful-restart

Configures graceful-restart. By default, this capability is set to enabled.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] capability graceful-restart
```

no

Disables the graceful-restart capability.

default

Enables the graceful-restart capability if it has been disabled.

Usage

Use this command to configure graceful-restart.

Example

The following command configures graceful-restart:

```
capability graceful-restart
```

default-information originate

Creates a default external route into an OSPF routing domain.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

default-information originate

default-information originate [**always**] [**metric** *metric_value*] [**metric-type** { **1** | **2** }] [**route-map** *route_map_name*]

no default-information originate

no

Disables the default external route.

always

Always advertise the route regardless of whether or not the software has a default route.

metric *metric_value*

Sets the OSPF metric used in creating the default rout as an integer from 1 through 16777214.

metric-type { 1 | 2 }

Sets the default route metric type.
1: Sets the OSPF external link type for default routes to Type 1.
2: Sets the OSPF external link type for default routes to Type 2.

route-map *route_map_name*

Specifies the name of the default route-map to be use as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to set the default external route into an OSPF routing domain.

Example

The following command sets the default external route to originate from the route map named *rmap1*:

default-information originate route-map rmap1

default metric

Configures the default metric value for the OSPF routing protocol.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

default-metric *metric_value*

no default-metric

metric-value

Sets the metric value expressed as an integer from 1 through 16777214. The default metric value setting is 26385.

no

Enables or disables the default metric value for OSPF.

Usage

Use this command to set the default metric for routes.

Example

The following command sets the default metric to *235*:

default-metric 235

distance

Configures the OSPF route administrative distances for all OSPF route types or based on specific route type. Administrative distance is the measure used by Cisco routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) using an administrative distance value. A lower numerical value is preferred.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] distance { distance_value | ospf { [ external distance_value ] [ inter-area
distance_value ] [ intra-area distance_value ] } }
```

no

Disables the OSPF route administrative distances for all OSPF route types.

distance_value

Specifies the OSPF route administrative distances as an integer from 1 to 255. The default distance value is 110.

ospf { [external *distance_value* **] [inter-area** *distance_value* **] [intra-area** *distance_value* **] }**

Set the distance value for the specified route type.
external *distance_value*: Set the OSPF route administrative distance for routes from other routing domains, learned by redistribution. This must be an integer from 1 through 255. The default is 110.
inter-area *distance_value*: sets the OSPF route administrative distance for routes from one routing area to another. This must be an integer from 1 through 255. The default is 110.
intra-area *distance_value*: sets the OSPF route administrative distance for all routes within an area. This must be an integer from 1 through 255. The default is 110.

no

Enables or disables the specified option.

Usage

Use this command to set the administrative distance for OSPF routes.

Example

The following command sets the administrative distance for all OSPF route types to *30*:

```
distance 30
```

distribute-list

Enables or disables the filtering of networks in outgoing routing updates.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] distribute-list route_access_list out { connected | rip | static }
```

no

Disables the filtering of networks in outgoing routing updates.

route_access_list

Specifies the name of the OSPF route access list to use for filtering as an alphanumeric string of 1 through 63 characters.

connected

Filters connected routes.

rip

Filters RIP routes. (RIP is not supported at this time.)

static

Filters static routes.

no

Disables the specified option.

Usage

Use this command to enable the filtering of outgoing route updates by using the specified route access list.

Example

The following command uses the route access list named *ral1* to filter outgoing routing updates for all connected routes:

```
distribute-list ral1 out connected
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

ip vrf

Configures the Virtual Routing and Forwarding (VRF) instances for OSPF routing protocol.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ip vrf vrf_name
```

no

Disables the VRF instances and removes the configured VRF context association for OSPF routing.

vrf*vrf_name*

Configures Virtual Routing & Forwarding (VRF) parameters.
vrf_name is name of a preconfigured VRF context configured in Context Configuration Mode via the **ip vrf** command. It is an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the IP VRF forwarding also to associate the preconfigured VRF context with the specific tunnel interface.
This command creates and enters the OSPF VRF Configuration Mode if required to configure the VRF context instances for OSPF routing.

Example

The following command enables preconfigured VRF context instance *ospf_vrf1* for OSPF routing and enters the OSPF VRF Configuration mode:

```
ip vrf ospf_vrf1
```

neighbor

Configures OSPF routers that interconnect to non-broadcast networks.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] neighbor  ip_address  [ poll-interval poll_interval_value ] [ priority
priority_value ]
```

no

Disables OSPF routers that interconnect to non-broadcast networks.

ip_address

Specifies the interface IP address of the OSPF neighbor expressed using IPv4 dotted-decimal notation.

poll-interval *poll_interval_value*

Default: 120
Sets the number of seconds in the dead neighbor polling interval as an integer from 1 through 65535

priority *priority_value*

Default: 0
Sets the 8-bit number that represents the router priority value of the non-broadcast neighbor associated with the specified IP address. This must be an integer from 0 through 255. This keyword does not apply to point-to-multipoint interfaces.

Usage

Use this command to configure OSPF routers that connect to non-broadcast networks.

Example

The following command specifies an OSPF router neighbor with the IP address of *192.168.100.10*:

```
neighbor 192.168.100.10
```

network area

Enables OSPF on an interface and defines the OSPF area for that network.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] network network_ip_address / network_mask area { area_id | area_ip_address }
```

no

Disables OSPF on an interface and defines the OSPF area for that network.

network_ip_address/network_mask

Specifies the network address and mask as well as the interface on which OSPF will be enabled. *network_ip_address* in entered in IPv4 dotted-decimal notation, followed by the "/" and the mask (CIDR).

area_id

Specifies the OSPF area identification number for the specified network as an integer from 0 through 4294967295.

area_ip_address

Specifies the IP address of the OSPF area for this network. This must be entered in IPv4 dotted-decimal notation.

Usage

Use this command to specify the IP address of the network interface that the OSPF router will use.

Example

The following command specified that the OSPF router will use the interface at IP address *192.168.1.0* with a netmask of *24*:

```
network 192.168.1.0/24
```

ospf graceful-restart

Configures OSPF graceful-restart settings.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

ospf graceful-restart { **grace-period** *grace_period* | **helper** { **never** | **policy** { **only-reload** | **only-upgrade** } } }

grace-period grace-period

Specifies the OSPF graceful restart grace period (in seconds) as an integer from 1 through 1800. Default grace period is 60 seconds.

helper { never | policy { only-reload | only-upgrade } }

Helps configure OSPF helper settings.
never: Do not allow helper mode.
policy { only-reload | only-upgrade }: Allows ospf graceful-restart helper mode.

- **only-reload**: Allows ospf graceful-restart helper mode only for a reload.
- **only-upgrade**: Allows ospf graceful-restart helper mode only for an upgrade.

Default is ospf graceful-restart grace-period.

Usage

Use this command to configure graceful-restart specific settings.

Example

The following command sets the graceful restart grace period to *60* seconds:

```
ospf graceful-restart grace-period 60

ospf graceful-restart helper policy only-reloadL

ospf graceful-restart helper policy only-upgrade
```

ospf router-id

This command configures the router ID for the OSPF process.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ospf router-id  ip_address
```

no

Disables the router ID for the OSPF process.

router-id *ip_address*

Specifies the router ID for the OSPF process. *ip_address* is entered using IPv4 dotted-decimal notation.

Usage

Use this command to set the router ID for the current OSPF router process.

Example

The following command sets the router ID to *192.168.200.1*:

```
ospf router-id 192.168.200.1
```

passive-interface

Enables or disables the suppression of OSPF routing updates on the specified interface.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] passive-interface interface_name
```

no

Disables the name assigned to a logical interface within the specific context.

interface_name

Specifies the name assigned to a logical interface within the specific context as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to suppress router updates on an interface in the current context.

Example

The following command suppresses OSPF routing updates on the interface named *Intfc1*:

```
passive-interface Intfc1
```

redistribute

Redistributes routes from other protocols to OSPF neighbors using the OSPF protocol.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

redistribute { **connected** | **rip** | **static** } [**metric** *metric_value*] [**metric-type** { **1** | **2** }] [**route-map** *route_map_name*]

no redistribute { **connected** | **rip** | **static** }

no

Disables the redistributed routes.

connected

Redistributes connected routes.

rip

Specifies that RIP routes will be redistributed. (RIP is not supported at this time.)

static

Redistributes static routes.

metric *metric_value*

Sets the OSPF metric used in the redistributed route. This must be an integer from 1 through 16777214.

metric-type { 1 | 2 }

Default: 2
Sets route metric type that is applied to redistributed routes.
1: Sets the OSPF external link type for routes to Type 1.
2: Sets the OSPF external link type for routes to Type 2.

route-map *route_map_name*

Filter routes through the specified route map before redistribution. *route_map_name* specifies the name of the route-map to use as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to define what routing protocols should have their routes redistributed into OSPF.

Example

The following command defines that BGP routes should be redistributed:

```
redistribute connected
```

refresh timer

Adjusts settings for the OSPF refresh timer.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] refresh  timer value
```

no

Disables the refresh timer.

value

Default: 10
Specifies the minimum amount of time (in seconds) to wait before refreshing a Link-state Advertisement (LSA). This must be an integer from 10 through 1800.

Usage

Use this command to define the amount of time to wait before refreshing an LSA.

Example

The following command sets the refresh timer to *90* seconds:

```
refresh timer 90
```

router-id

Configures the router ID for the OSPF process.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] router-id ip_address
```

no

Disables the router ID for the OSPF process.

ip_address

Specifies the router ID for the OSPF process in IPv4 dotted-decimal notation.

Usage

Use this command to set the router ID for the current OSPF router process.

Example

The following command sets the router ID to *192.168.200.1*:

```
router-id 192.168.200.1
```

timers spf

Sets the Shortest Path First (SPF) timers.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

timers spf *delay_value hold_time_value*

no timers spf

no

Disables SPF timers.

delay_value

Default: 5
Specifies the delay time (in seconds) between receiving changes to an SPF calculation. This must be an integer from 0 through 4294967295.

hold_time_value

Default: 10
Specifies the hold time (in seconds) between consecutive SPF calculations. This must be an integer from 0 through 4294967295.

Usage

Use this command to set the SPF delay and hold timers for the current OSPF router process.

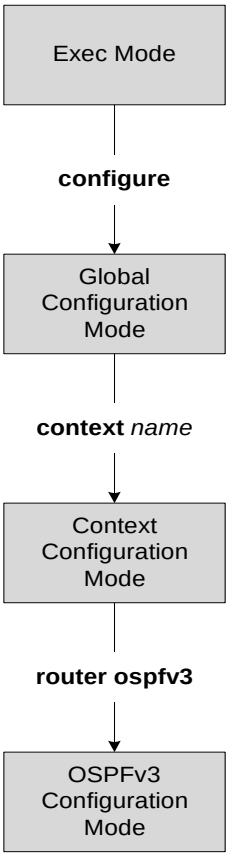
Example

The following command sets the delay timer to *15* and the hold timer to *15*:

```
timers spf 15 15
```

Chapter 212
OSPFv3 Configuration Mode Commands

The OSPFv3 Configuration sub-mode is used to configure the OSPFv3 routing protocol. This mode includes commands that configure OSPFv3 routing parameters.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

area

Configures an Open Shortest Path First Version 3 (OSPFv3) area and enables authentication for that area.

Product

PDSN, HA GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] area { decimal_value | ipv4address } default-cost default_integer_value | stub [
no-summary ] | virtual-link virtuallink_neighbour_Ipv4_address [ dead-interval
virtuallink_dead_interval ] [ hello-interval virtuallink_hello_interval ] [ retransmit-
interval virtuallink_retransmit_interval ] [ transmit-delay virtuallink_transmit_delay ]
```

no

Disables authentication for the specified area.

decimal_value|*ipv4address*

decimal_value: Specifies the identification number of the area where authentication will be enabled as an integer from 0 through 4294967295.

ipv4address: Specifies the IP address of the area where authentication will be enabled in IPv4 dotted-decimal notation.

default-cost *default_integer_value*

Sets the OSPFV3 authentication area's default cost as an integer from 1 through 16777215.

stub [no-summary]

Sets the OSPFV3 stub area. Only Router-LSAs, Network-LSAs, Inter-area Prefix-LSAs, Intra-area Prefix-LSAs and Link-LSAs are allowed in a Stub area.

no-summary Does not inject inter-area routes into stub area.

virtual-link *virtuallink_neighbour_Ipv4_address*

Configures a virtual link to the authentication area.

virtuallink_neighbour_Ipv4_address is the IPv4 address for the virtual link of the authenticated area in dotted-decimal notation.

The following interval timers can be set for the virtual link:

- **dead-interval** *virtuallink_dead_interval*: Sets the virtual link dead-interval (in seconds) as an integer from 1 through 65535.
- **hello-interval** *virtuallink_hello_interval*: Sets the virtual link hello interval (in seconds) as an integer from 1 through 65535.
- **retransmit-interval** *virtuallink_retransmit_interval*: Sets the virtual link retransmit interval (in seconds) as an integer from 1 through 3600.

- **transmit-delay** *virtuallink_transmit_delay*: Sets the virtual link transmit delay (in seconds) as n integer from 1 through 3600.

Usage

Use this command to establish OPSFv3 areas and enable authentication.

Example

The following command enables authentication for an OSPFv3 area defined by the IP address *192.168.100.10* with default cost of *256*

```
area 192.168.100.10 default-cost 256
```

default-metric

Configures the default metric value for routes redistributed from another protocol into Open Shortest Path First Version 3 (OSPFv3).

Product

PDSN, HA GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ]  default-metric default_metric_integer_value
```

no

Disables the default metric.

default_metric_integer_value

Specifies the default metric as an integer from 1 through 16777214.

Usage

Use this command to configure OPSFv3 default metric.

Example

The following command configures OSPFv3 default metric to 256

```
default-metric 256
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

passive Interface

Configures an OSPFv3 passive interface as passive. If a network interface is configured as passive, it will not receive or send any OSPFv3 packets.

Product

PDSN, HA GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ]  passive-interface passive_interface_name
```

no

Disables the passive interface.

passive-interface *passive_interface_name*

Sets the named interface to be a passive interface as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to configure an OPSFv3 passive interface in this context.

Example

The following command configures an OSPFv3 passive interface.

```
passive-interface OSPF-if1
```

redistribute

Redistributes routes from other protocols to OSPFv3 neighbors using the OSPFv3 protocol.

Product

PDSN, HA GGSN

Privilege

Security Administrator, Administrator

Syntax

[no] redistribute { connected | static } redistribute connected [**metric** *metric_value* [**metric-type** *external_metric_type*] [**route-map** *route_map_name*]] [**metric-type** *external_metric_type* [**route-map** *route_map_name*]] [**route-map** *route_map_name*] **static** [**metric** *metric_value* [**metric-type** *external_metric_type*] [**route-map** *route_map_name*]] [**metric-type** *external_metric_type* [**route-map** *route_map_name*]] [**route-map** *route_map_name*]

no

Disables the route redistribution.

connected

Redistributes connected routes.

static

Redistributes static routes.

metric *metric_value*

Specifies the OSPFv3 default metric value as an integer from 0 through 16777214.

metric-type *external_metric_type*

Specifies the OSPFv3 external metric type as the integer 1 or 2

route-map *route_map_name*

Specifies a route map as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to configure OPSFv3 redistribution of connected or static routes.

Example

The following command configures OSPFv3 redistribution of connected routes.

```
redistribute connected metric 45 metric-type 1 route-map rt
```

router-id

Sets the OSPFv3 router ID for the Open Shortest Path First Version 3 (OSPFv3) routing process.

Product

PDSN, HA GGSN

Privilege

Security Administrator, Administrator

Syntax

[no] router-id *router_id_ipaddress*

no

Disables the router-id.

router_id_ipaddress

Specifies the router-id an IPv4 address in dotted-decimal notation.

Usage

Use this command to configure OPSF v3 router id to the given IPv4 address.

Example

The following command configures OSPFv3 router id to the given IPv4 address.

```
router-id 11.22.22.21
```

timers spf

Sets OSPFv3 the delay in the time between the detection of a topology change and when the SPF algorithm actually runs.

Product

PDSN, HA GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] timers spf spf_delay_timer_value
```

no

Disables the SPF delay timer.

spf *spf_delay_timer_value*

Sets the Shortest Path First (SPF) delay timer (in milliseconds) as an integer from 0 through 4294967295.

Usage

Use this command to configure the OPSFv3 SPF delay timer.

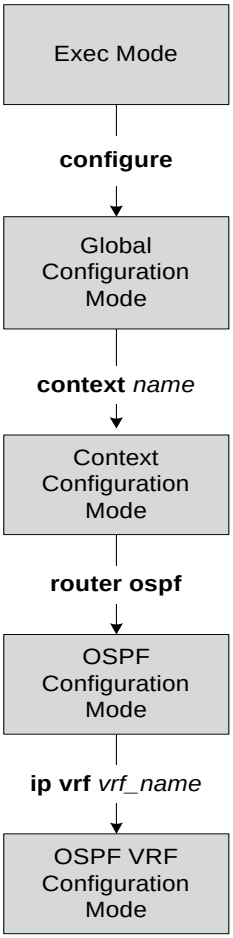
Example

The following command sets OSPFv3 SPF timer.

```
timers spf 256
```

Chapter 213
OSPF VRF Configuration Mode Commands

The OSPF VRF Configuration sub-mode is used to configure the virtual routing and forwarding (VRF) context instances for OSPF routing protocol. This mode includes commands that configure VRF instance for OSPF routing parameters.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

area

Configures various parameters, including authentication, area identification, virtual link ID, and delay/interval values for the specified OSPF area using a specific VRF instance.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

[no] area { *decimal_value* **|** *ip_address* **} {authentication [message-digest] | default-cost** *cost_value* **| nssa [default-information-originate] [no-redistribution] [no-summary] [translate-always] [translate-candidate] [translate-never] | stub [no-summary] | virtual-link** *router_ip_address* **[authentication {message-digest | null | text}| authentication-key {encrypted password** *encrypted_string* **| password** *password_string***}| message-digest-key** *key_id* **md5 [encrypted password** *encrypted_string* **| password** *password_string***]} [dead-interval] [hello-interval] [retransmit-interval] [transmit-delay]**

---

no

Disables or removes configured parameters for the specified OSPF area using a specific VRF instance.

---

ip_address

Specifies the IP address of the area where authentication will be enabled in IPv4 dotted-decimal notation.

---

decimal_value

Specifies the identification number of the area where parameters to be configured as an integer from 0 through 4294967295.

---

authentication

Sets the OSPF authentication type to use the simple authentication method.

---

message-digest

Sets the OSPF authentication type to use the message digest 5 (MD5) authentication method.

---

default-cost *cost_value*

Sets the default cost for an OSPF area. *cost_value* must be an integer from 0 through 16777215.

---

nssa [default-information-originate] [no-redistribution no-summary] [translate-always] [translate-candidate] [translate-never]

Configures and defines an area as an NSSA (Not So Stubby Area) and configures OSPF parameters for it.
default-information-originate: Configures the OSPF VRF instances to originate default information to the NSSA area.
no-redistribution: Configures the OSPF VRF instance to not to redistribute external routes to the NSSA area.
no-summary: Configures the OSPF VRF instance to not to inject the inter-area routes into NSSA.

translate-always: Configures the NSSA-ABR (Area Border Router) always to translate. By default this is disabled.
translate-candidate: Configures the NSSA-ABR always to translate election. By default this is enabled.
translate-never: Configures the NSSA-ABR never to translate. By default this is disabled.

---

stub [no-summary]

Specifies an OSPF area as an stub area configures the NSSA-ABR never to translate. By default this is disabled.
no-summary: Disables (stops) the ABR from sending summary LSAs into the stub area.

---

virtual-link *router_id*

Specifies the router identifier which provides a virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone. *router_id* must be an IP address in IPv4 dotted-decimal notation of the ABR to be linked to.

---

authentication {message-digest | null | text}

Configures the OSPF authentication method to be used by the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.
message-digest: Set the OSPF authentication type to use the message digest (MD) authentication method.
null: Set the OSPF authentication type to use no authentication, thus disabling either MD or clear text methods.
text: Set the OSPF authentication type to use the clear text authentication method.

---

authentication-key

Configures the authentication password for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

---

message-digest-key *key_id*

Specifies the MD key identifier number for virtual link connection. *key_id* must be an integer from 1 through 255.

---

md5

Sets the message digest to MD5 for virtual link connection.

[encrypted] password *passwd_string*

Specifies the password required for virtual link connection authentications. The keyword **password** is optional and if specified *passwd_string* must be an alphanumeric string of 1 through 63 characters. The password specified must be in an encrypted format if the optional keyword **encrypted** was specified.
The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file. *encrypted_string* is an alphanumeric string of 1 through 523 characters.

---

dead-interval *value*

Specifies the dead interval (in seconds) that the router should wait, during which time no packets are received and after the router considers a neighboring router to be off-line. *value* must be an integer from 1 through 65535.

hello-interval *value*

Specifies the hello interval (in seconds) before sending a hello packet. *value* must be an integer from 1 through 65535.

retransmit-interval *value*

Specifies the delay between retransmission (in seconds) that router should wait before retransmitting a packet. *value* must be an integer from 1 through 3600.

transmit-delay *value*

Specifies the interval (in seconds) that the router should wait before transmitting a packet. *value* must be an integer from 1 through 3600.

Usage

Use this command to configure/set the various network/connection/authentication parameters of OPSF areas using specific VRF instance.

Example

The following command enables authentication for an OSPF area defined by the IP address *192.168.100.10* and the OSPF authentication type to MD5:

```
area 192.168.100.10 authentication message-digest
```

The following command defines the area designated by the IP address *192.168.100.10* as an NSSA area where translation of NSSA candidate is enabled by default:

```
area 192.168.100.10 nssa
```

The following command defines the OSPF area defined by the IP address *192.168.100.10* as a stub area:

```
area 192.168.100.10 stub
```

The following command creates a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20*:

```
area 192.168.100.10 virtual-link 192.168.200.20
```

The following command sets the authentication method for a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20* to use no authentication:

```
area 192.168.100.10 virtual-link 192.168.200.20 null
```

The following command creates an authentication password of *123456* for a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20*:

```
area 192.168.100.10 virtual-link 192.168.200.20 authentication-key
password 123456
```

The following command enables the use of MD5-based OSPF authentication for a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20*, sets the MD5 Key ID to *25*, and the password to *123456*:

```
area 192.168.100.10 virtual-link 192.168.200.20 message-digest-key 25 md5
password 123456
```

The following command sets the retransmit interval for a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20* to *60* seconds:

```
area 192.168.100.10 virtual-link 192.168.200.20 retransmit-interval 60
```

default-information originate

Creates a default external route into an OSPF routing domain.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
default-information originate

default-information originate [ always ] [ metric metric_value ] [ metric-type { 1 | 2 } ] [ route-map route_map_name ]

no default-information originate
```

no

Disables the default external route.

always

Always advertise the route regardless of whether or not the software has a default route.

metric *metric_value*

Sets the OSPF metric used in creating the default rout as an integer from 1 through 16777214.

metric-type { 1 | 2 }

Sets the default route metric type.
1: Sets the OSPF external link type for default routes to Type 1.
2: Sets the OSPF external link type for default routes to Type 2.

route-map *route_map_name*

Specifies the name of the default route-map to be use as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to set the default external route into an OSPF routing domain.

Example

The following command sets the default external route to originate from the route map named *rmap1*:

```
default-information originate route-map rmap1
```

default metric

Configures the default metric value for the OSPF routing protocol.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

default-metric *metric_value*

no default-metric

metric-value

Sets the metric value expressed as an integer from 1 through 16777214. The default metric value setting is 26385.

no

Enables or disables the default metric value for OSPF.

Usage

Use this command to set the default metric for routes.

Example

The following command sets the default metric to *235*:

```
default-metric 235
```

distance

Configures the OSPF route administrative distances for all OSPF route types or based on specific route type. Administrative distance is the measure used by Cisco routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) using an administrative distance value. A lower numerical value is preferred.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] distance { distance_value | ospf { [ external distance_value ] [ inter-area
distance_value ] [ intra-area distance_value ] } }
```

no

Disables the OSPF route administrative distances for all OSPF route types.

distance_value

Specifies the OSPF route administrative distances as an integer from 1 to 255. The default distance value is 110.

ospf { [external *distance_value* **] [inter-area** *distance_value* **] [intra-area** *distance_value* **] }**

Set the distance value for the specified route type.
external *distance_value*: Set the OSPF route administrative distance for routes from other routing domains, learned by redistribution. This must be an integer from 1 through 255. The default is 110.
inter-area *distance_value*: sets the OSPF route administrative distance for routes from one routing area to another. This must be an integer from 1 through 255. The default is 110.
intra-area *distance_value*: sets the OSPF route administrative distance for all routes within an area. This must be an integer from 1 through 255. The default is 110.

no

Enables or disables the specified option.

Usage

Use this command to set the administrative distance for OSPF routes.

Example

The following command sets the administrative distance for all OSPF route types to *30*:

```
distance 30
```

distribute-list

Enables or disables the filtering of networks in outgoing routing updates.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] distribute-list route_access_list out { connected | rip | static }
```

no

Disables the filtering of networks in outgoing routing updates.

route_access_list

Specifies the name of the OSPF route access list to use for filtering as an alphanumeric string of 1 through 63 characters.

connected

Filters connected routes.

rip

Filters RIP routes. (RIP is not supported at this time.)

static

Filters static routes.

no

Disables the specified option.

Usage

Use this command to enable the filtering of outgoing route updates by using the specified route access list.

Example

The following command uses the route access list named *ral1* to filter outgoing routing updates for all connected routes:

```
distribute-list ral1 out connected
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

neighbor

Configures OSPF routers that interconnect to non-broadcast networks.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] neighbor  ip_address  [ poll-interval poll_interval_value ] [ priority
priority_value ]
```

no

Disables OSPF routers that interconnect to non-broadcast networks.

ip_address

Specifies the interface IP address of the OSPF neighbor expressed using IPv4 dotted-decimal notation.

poll-interval *poll_interval_value*

Default: 120
Sets the number of seconds in the dead neighbor polling interval as an integer from 1 through 65535

priority *priority_value*

Default: 0
Sets the 8-bit number that represents the router priority value of the non-broadcast neighbor associated with the specified IP address. This must be an integer from 0 through 255. This keyword does not apply to point-to-multipoint interfaces.

Usage

Use this command to configure OSPF routers that connect to non-broadcast networks.

Example

The following command specifies an OSPF router neighbor with the IP address of *192.168.100.10*:

```
neighbor 192.168.100.10
```

network area

Enables OSPF on an interface and defines the OSPF area for that network.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] network network_ip_address / network_mask area { area_id | area_ip_address }
```

no

Disables OSPF on an interface and defines the OSPF area for that network.

network_ip_address/network_mask

Specifies the network address and mask as well as the interface on which OSPF will be enabled. *network_ip_address* in entered in IPv4 dotted-decimal notation, followed by the "/" and the mask (CIDR).

area_id

Specifies the OSPF area identification number for the specified network as an integer from 0 through 4294967295.

area_ip_address

Specifies the IP address of the OSPF area for this network. This must be entered in IPv4 dotted-decimal notation.

Usage

Use this command to specify the IP address of the network interface that the OSPF router will use.

Example

The following command specified that the OSPF router will use the interface at IP address *192.168.1.0* with a netmask of *24*:

```
network 192.168.1.0/24
```

ospf router-id

Configures the router ID for the OSPF process.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

ospf router-id *ip_address*

no ospf router-id *ip_address*

no

Disables **ospf router-id**.

ip_address

Specifies the router ID for the OSPF process as an IP address entered using IPv4 dotted-decimal notation

Usage

Use this command to set the router ID for the current OSPF router process.

Example

The following command sets the router ID to *192.168.200.1*:

```
ospf router-id 192.168.200.1
```

passive-interface

Enables or disables the suppression of OSPF routing updates on the specified interface.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

[no] passive-interface *interface_name*

no

Disables the name assigned to a logical interface within the specific context.

interface_name

Specifies the name assigned to a logical interface within the specific context as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to suppress router updates on an interface in the current context.

Example

The following command suppresses OSPF routing updates on the interface named *Intfc1*:

```
passive-interface Intfc1
```

redistribute

Redistributes routes from other protocols to OSPF neighbors using the OSPF protocol.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

redistribute { **connected** | **rip** | **static** } [**metric** *metric_value*] [**metric-type** { **1** | **2** }] [**route-map** *route_map_name*]

no redistribute { **connected** | **rip** | **static** }

no

Disables the redistributed routes.

connected

Redistributes connected routes.

rip

Specifies that RIP routes will be redistributed. (RIP is not supported at this time.)

static

Redistributes static routes.

metric *metric_value*

Sets the OSPF metric used in the redistributed route. This must be an integer from 1 through 16777214.

metric-type { 1 | 2 }

Default: 2
Sets route metric type that is applied to redistributed routes.
1: Sets the OSPF external link type for routes to Type 1.
2: Sets the OSPF external link type for routes to Type 2.

route-map *route_map_name*

Filter routes through the specified route map before redistribution. *route_map_name* specifies the name of the route-map to use as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to define what routing protocols should have their routes redistributed into OSPF.

Example

The following command defines that BGP routes should be redistributed:

```
redistribute connected
```

refresh timer

Adjusts settings for the OSPF refresh timer.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] refresh  timer value
```

no

Disables the refresh timer.

value

Default: 10
Specifies the minimum amount of time (in seconds) to wait before refreshing a Link-state Advertisement (LSA). This must be an integer from 10 through 1800.

Usage

Use this command to define the amount of time to wait before refreshing an LSA.

Example

The following command sets the refresh timer to *90* seconds:

```
refresh timer 90
```

router-id

Configures the router ID for the OSPF process.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] router-id ip_address
```

no

Disables the router ID for the OSPF process.

ip_address

Specifies the router ID for the OSPF process in IPv4 dotted-decimal notation.

Usage

Use this command to set the router ID for the current OSPF router process.

Example

The following command sets the router ID to *192.168.200.1*:

```
router-id 192.168.200.1
```

timers spf

Sets the Shortest Path First (SPF) timers.

Product

PDSN, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

timers spf *delay_value hold_time_value*

no timers spf

no

Disables SPF timers.

delay_value

Default: 5
Specifies the delay time (in seconds) between receiving changes to an SPF calculation. This must be an integer from 0 through 4294967295.

hold_time_value

Default: 10
Specifies the hold time (in seconds) between consecutive SPF calculations. This must be an integer from 0 through 4294967295.

Usage

Use this command to set the SPF delay and hold timers for the current OSPF router process.

Example

The following command sets the delay timer to *15* and the hold timer to *15*:

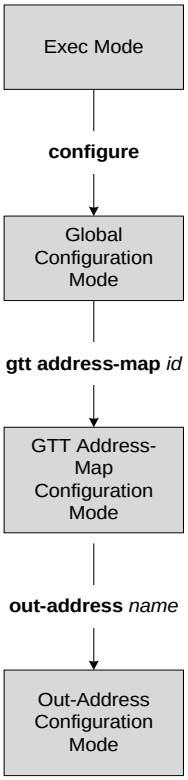
```
timers spf 15 15
```

Chapter 214
Out-Address Configuration Mode Commands

The Out-Address configuration mode provides the commands to configure the outgoing addresses for SCCP entities.

In this mode, the prompt line will appear similar to:

```
[local]hostname(config-gtt-addrmap-outaddr-<name>)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the configuration mode and returns to the Global configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Return to the Global configuration mode.

gt-address

Configures the SCCP short address.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gt-address *gt_address*

gt_address

A string of 1 to 15 digits to define the GT-address

Usage

Define the GT-address

Example

gt-address *010405525397*

gt-format

The GT-format provides four formats that can be used during GTT.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gt-format *format_num*

format_num

1: Selects GT-format 1 options which include **nature-of-address** and **odd/even.** Once selected, the system enters GT-Format1 configuration mode.
2: Selects GT-format2 options which include **translation-type**. Once selected, the system enters GT-Format2 configuration mode.
3: Selects GT-format3 options which include **encoding-scheme**, **numbering-plan3** and **translation-type**. Once selected, the system enters GT-Format1 configuration mode.
4: Selects GT-format4 options which include **encoding-scheme**, **nature-of-address**, **numbering-plan**, and **translation-type**. Once selected, the system enters GT-Format4 configuration mode.

Usage

Select the a GT-format that include encoding-scheme as part of the GTT process.

Example

```
gt-format 3
```

ni-indicator

Configures the National and International indicator to use during the GTT process.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ni-indicator *ni_ind*

ni_ind

Select one of the following as the appropriate type of national indicator for the address structure:

- **national**
- **international**

Usage

Select the international indicator to be used for out-going addresses.

Example

ni-indicator *international*

point-code

Selects and configures the SS7-type point code for use with the out-going address.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

point-code *pt_code*

pt_code

Enter 1 to 11 digits in the point code format predefined during variant selection of GTT association.

Usage

Define an ITU point code to be used for out-going address processing.

Example

point-code *6.255.6*

routing-indicator

Selects the type of routing and the indicator to be included in the out-going message.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

routing-indicator *routing_ind*

routing_ind

Select one of the following options:

- **gt**: Inserts an indicator that identifies routing based on global title.
- **ssn**: Inserts an indicator that identifies routing based on the subsystem number.

Usage

Select global title as the appropriate routing indicator.

Example

routing-indicator *gt*

ssf

Selects the subservice field as factor in the out-going address processing. **ssf** sets the network indicator in the subservice field for SS7 Message Signal Units (MSUs). The indicator carried in the message's routing information typically identifies the structure of the point code as a message from within a nation or as a message coming from outside the national - international.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ssf *sub_svc_fld*

sub_svc_fld

Select one of the following options:

- **international:** The network indicator identifies the message as international with a point code structure that does not match the national point code structure,
- **national:** The network indicator identifies the messages as having a national point code structure.
- **reserved:** Provides an alternate network indicator for national messages.
- **spare:** Provides an alternate network indicator for international messages.

Usage

Select the international NI for inclusion in out-going address subservice fields.

Example

ssf *international*

ssn

Selects the subsystem number to be included in the out-going message.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ssn *sub_sys_num*

sub_sys_num

Enter an integer from 1 to 255.

Usage

Use subsystem number 44 in the out-going address.

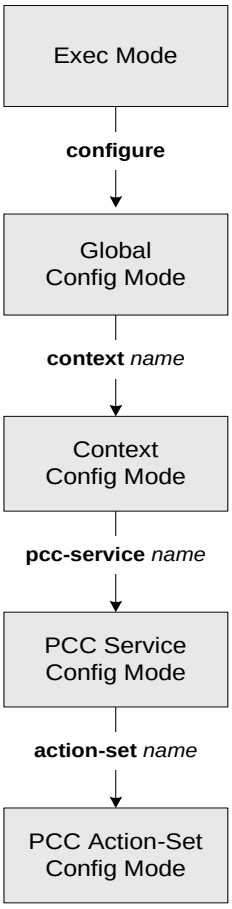
Example

ssn *44*

Chapter 215
PCC-Action-Set Configuration Mode Commands

The PCC- Action-Set Configuration Mode provides the parameters to indicate the policy and charging as well as event generation related decisions that will get activated when the corresponding PCC-Condition-Group is evaluated to TRUE within a profile. A maximum of 32 actions can be configured in an instance of PCC-Action-Set.

Important: This configuration mode is supported from StarOS Release 12.1 onward.



af-media-type

This command is used to set the action to be taken when specific media type is received from Application Function (AF) over Rx interface.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] af-media-type {application | audio | control | data | message | other | text |
video} {qos-profile qos_profile_value [gate-status {disabled | enabled | enabled-downlink
| enabled-uplink]} {gate-status {disabled | enabled | enabled-downlink | enabled-uplink
[qos-profile qos_profile_value]}
```

no

Removes the configured action set for different type of AF media in a PCC-Action-Set configuration instance for PCC-Service configuration.

application

Sets the AF media type to ‘application’ data traffic for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

audio

Sets the AF media type to ‘audio’ data traffic for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

control

Sets the AF media type to ‘control’ signal for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

data

Sets the AF media type to ‘data’ for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

message

Sets the AF media type to ‘message’ data for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

other

Sets the AF media type to ‘other’, out of AF media type configured here, for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

text

Sets the AF media type to 'text' for various action configured under PCC-Action-Set configuration instance for PCC-Service configuration.

video

Sets the AF media type to 'video' for various action configured under PCC-Action-Set configuration instance for PCC-Service configuration.

qos-profile *qos_profile_value*

Associate the pre-defined PCC-QoS-Profile for specific AF media type for various action configured for PCC-Service configuration.
qos_profile_value is name of the pre-defined PCC-QoS-Profile in PCC-Service Configuration instance.

gate-status {disabled | enabled | enabled-downlink | enabled-uplink}

Default: Enabled
Associate the status of Gate for specific AF media type for various action configured for PCC-Service configuration.
disabled: disables the Gate status in downlink and uplink direction for specific type of AF media type along optionally with PCC-QoS-Profile in PCC-Service Configuration instance.
enabled: Enables the Gate status in downlink and uplink direction for specific type of AF media type along optionally with PCC-QoS-Profile in PCC-Service Configuration instance. This is the default status of Gate.
enabled-downlink: Enables the Gate status in downlink direction for specific type of AF media type along optionally with PCC-QoS-Profile in PCC-Service Configuration instance.
enabled-uplink: Enables the Gate status in uplink direction for specific type of AF media type along optionally with PCC-QoS-Profile in PCC-Service Configuration instance.

Usage

Use this command to set the action to be taken when specific media type is received from Application Function (AF) over Rx interface.
It also associates the pre-defined PCC-QoS-Profile and **Gate** function with specific media type.

Example

The following command sets the AF media type to 'video' with PCC-QoS-Profile named *video_qos1* with gate status enabled in downlink and uplink traffic for various action configured under PCC-Action-Set configuration instance for PCC-Service configuration:

```
af-media-type video qos-profile video_qos1 gate-status enabled
```

associate monitoring-key

This command associates a Monitoring Key id with a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] associate monitoring-key mon_key_id usage-monitor usage_mon_name
```

no

Removes the associated Monitoring Key id configuration along with the association to PCC-Usage-Monitor from a PCC-Action-Set configuration instance for PCC-Service configuration.

mon_key_id

Specifies the Monitoring Key identifier to be associated with PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.
mon_key_id must be an integer between 1 through 65535.

usage-monitor *usage_mon_name*

Specifies the PCC-Usage-Monitor associated with Monitoring Key *mon_key_id* under PCC-Action-Set configuration instance for PCC-Service configuration.
usage_mon_name is a pre-configured PCC-Usage-Monitor instance in PCC-Service Profile Configuration for PCC-Service configuration.

Usage

Use this command to associate a Monitoring Key with a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.
There is a Many-To-Many relationship between Usage-Monitor and Monitoring-Key. Operator can change this relationship using required command.
When usage is reported to IPCF for a particular Monitoring Key, the usage is added to all the Usage Monitoring to which the Monitoring Key is associated.
Operator can break the relationship between Monitoring Key and Usage Monitor by **dissociate monitoring-key** command.

Example

The following command associates Monitoring Key id *102* with pre-defined PCC-Usage-Monitor named *usage_mon1* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
associate monitoring-key 102 usage-monitor usage_mon1
```

authorize

This command sets an action to change the various authorization parameters used for the IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] authorize {apn-mbr | default-eps-bearer | qci qci_value} qos-profile qos_prof_name
```

no

Removes the configured action for QoS Profile authorization parameters from PCC-Action-Set configuration instance for PCC-Service configuration.

apn-mbr

Sets the action for QoS authorization of Maximum Bit Rate (MBR) at APN through a pre-configured QoS profile name *qos_prof_name* which is to use for the authorization at different level in an PCC-Service instance.
This keyword is applicable only to EPS access type. MBR Download and MBR Upload values of the QoS profile is used with this authorization.

default-eps-bearer

Sets the action QoS authorization of the Default EPS bearer in an EPS access network through a pre-configured QoS profile name *qos_prof_name* which is to use for the authorization at different level in an PCC-Service instance.
This keyword is applicable only to EPS access type. QoS Class Identifier (QCI) and Allocation and Retention Priority (ARP) values of the QoS profile is used with this authorization.

qci *qci_value*

Sets the action QoS authorization per QCI in case of PCEF binding through a pre-configured QoS profile name *qos_prof_name* which is to use for the authorization at different level in an PCC-Service instance. *qci_value* must be an integer value between 1 through 255.

Important: This keyword is applicable only in case of PCEF binding. QCI defined in QoS profile is not used when this keyword is active, so this keyword is repeated per QCI that has to be authorized by IPCF. For each QCI authorization Maximum Bit Rate Upload/Download (MBR DL/MBR UL) or Guaranteed Bit Rate Upload/Download (GBR DL/MBR UL) and ARP values of the QoS profile is used with this authorization.

qos-profile *qos_prof_name*

This keyword associate the action configured for authorization with a pre-configured PCC-QoS-Profile named *qos_prof_name* and uses configured values from specific PCC-QoS-Profile during authorization. *qos_prof_name* specifies the pre-configured QoS profile name which is to use for the authorization at different level in an PCC-Service instance.

Usage

Use this command to define an action for the authorization parameters in PCC-QoS-Profile which is to be used under PCC-Action-Set configuration instance for PCC-Service configuration.

Example

Following command sets the action for QoS authorization for APN MBR with PCC-QoS-Profile *apn_qos_prof1* under PCC-Action-Set configuration instance for PCC-Service configuration.

```
authorize apn-mbr qos-profile apn_qos_prof1
```

dissociate monitoring-key

This command dissociates a Monitoring Key id with a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

[no] dissociate monitoring-key *mon_key_id* **usage-monitor** *usage_mon_name*

no

Removes the dissociated Monitoring Key id configuration from a PCC-Action-Set configuration instance for PCC-Service configuration.

mon_key_id

Specifies the Monitoring Key identifier to be dissociated with PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.
mon_key_id must be an integer between 1 through 65535.

usage-monitor *usage_mon_name*

Specifies the PCC-Usage-Monitor need to be dissociated with Monitoring Key *mon_key_id* under PCC-Action-Set configuration instance for PCC-Service configuration.
usage_mon_name is a pre-configured PCC-Usage-Monitor instance in PCC-Service Profile Configuration for PCC-Service configuration.

Usage

Use this command to dissociate a Monitoring Key with a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.
There is a Many-To-Many relationship between Usage-Monitor and Monitoring-Key. Operator can change this relationship using required commands.
When usage is reported to IPCF for a particular Monitoring Key, the usage is added to all the Usage Monitoring to which the Monitoring Key is associated.
Operator can reassociate the relationship between Monitoring Key and Usage Monitor by **associate monitoring-key** command.

Example

The following command dissociates a associated pair of Monitoring Key id *102* and PCC-Usage-Monitor named *usage_mon1* under PCC-Action-Set configuration instance for PCC-Service configuration:

dissociate monitoring-key *102* **usage-monitor** *usage_mon1*

dynamic-rule-install

This command sets an action to install a PCC Dynamic rule for the specified PCC-Data-service in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] dynamic-rule-install data-service data_svc_name [qos-profile qos_prof_name]
[precedence preced_value] [monitoring-key mon_key_id [rating-group rating_grp_id] [gate-
status {disabled | enabled | enabled-downlink | enabled-uplink}] [defer-by interval
delayed_dur] [metering-method {both-duration-volume | duration | volume}] [reporting-
level {service-identifier-level | rating-group-level}] [failure-policy { continue |
terminate}]
```

no

Removes the Dynamic Rule install action configured for specific PCC-Data-Service from a PCC-Action-Set configuration instance for PCC-Service configuration.

data-service *data_svc_name*

Specifies the name of the pre-configured PCC-Data-Service for which Dynamic Rules to be installed under PCC-Action-Set configuration instance for PCC-Service configuration.
data_svc_name is a pre-configured PCC-Data-Service instance in PCC-Service Configuration mode.

metering-method {both-duration-volume | duration | volume}

Specifies the reporting level to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-service instance on IPCF node.

- **both-duration-volume** sets the metering method as based on volume of data usage and duration of session, both for offline charging in a PCC-Data-service instance on IPCF node.
- **duration** sets the metering method as based on duration of session usage for offline charging in a PCC-Data-service instance on IPCF node.
- **volume** sets the metering method as based on the volume of data usage for offline charging in a PCC-Data-service instance on IPCF node.

If no metering method is defined, the reporting level preconfigured at PCEF is considered.

monitoring-key *mon_key_id*

Specifies the pre-defined Monitoring Key identifier which is to be used in Dynamic Rule for specific PCC-Data-service under PCC-Action-Set configuration instance for PCC-Service configuration.
mon_key_id is a pre-defined Monitoring Key identifier in PCC-Service Configuration mode.

precedence *preced_value*

Specifies the precedence value for the Dynamic Rule for specific PCC-Data-service under PCC-Action-Set configuration instance for PCC-Service configuration.

preced_value must be an integer between 1 through 65535.

qos-profile *qos_prof_name*

Specifies the name of the pre-configured PCC-QoS-Profile which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.
qos_prof_name is a pre-configured PCC-QoS-Profile instance in PCC-Service Configuration mode.

rating-group *rating_grp_id*

Specifies the pre-defined Rating Group identifier which is to be used in Dynamic Rule for specific PCC-Data-service under PCC-Action-Set configuration instance for PCC-Service configuration.
rating_grp_id is a pre-defined Rating Group identifier in PCC-Service Configuration mode.

reporting-level {service-identifier-level | rating-group-level

Specifies the reporting level to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-service instance on IPCF node.

- **service-identifier-level** sets the data usage reporting level to be used by PCEF to report the data usage for the related PCC rule at the Service Identifier level which is configured in a PCC-Data-service instance on IPCF node.
- **rating-group-level** sets the data usage reporting level to be used by PCEF to report the data usage for the related PCC rule at the Rating Group level which is configured in a PCC-Data-service instance on IPCF node.

If no reporting level is defined, the reporting level preconfigured at PCEF is considered.

gate-status {disabled | enabled | enabled-downlink | enabled-uplink}

Default: Enabled
Sets the Gate-status which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.
disabled: disables the Gate status in downlink and uplink direction which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.
enabled: Enables the Gate status in downlink and uplink direction which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration. This is the default status of Gate.
enabled-downlink: Enables the Gate status in downlink direction which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.
enabled-uplink: Enables the Gate status in uplink direction which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.

defer-by interval *delayed_dur*

This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for dynamic rule installation.
delayed_dur configures the relative delay time by which the corresponding dynamic rule installation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed.
delayed_dur specifies the delayed interval in *HH MIN SS* format.
Following format is used for *HH MIN SS* in *delayed_dur*:

- *HH* specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- *MIN* specifies the minutes to defer the action trigger and must be an integer between 00 through 59.

- *ss* specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

failure-policy { continue | terminate}

Default: Continue
This optional keyword configures the rule failure policy action when failure occurs on PCEF for PCC rules.

- **Continue**: If this option enabled, the IPCF continues even if PCEF reports rule failure through charging rule report. This is the default action.
- **Terminate**: If this option enabled, the IPCF triggers PCC session termination on receiving rule failure through charging rule report.

Usage

Use this command to set an action to install a PCC Dynamic rule for the specified PCC-Data-Service in PCC-Action-Set configuration for PCC-Service instance
Operator can override parameters such as, QoS profile, Precedence, Gate-status, Monitoring Key and PCC-Rating-id.
The same command is used to modify already installed PCC Dynamic-rule for the PCC-Data-Service by overriding required parameters only.
Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding dynamic rule installation is deferred.
IPCF handles operation of PCC Rule and activate/deactivate/install/modify/remove the PCC rules at PCEF through this configuration. PCC rule operation may fail on PCEF due to various reasons. In such failure cases PCEF sends back a Charging Rule Report containing name of the failed PCC rule and corresponding failure cause.
The IPCF handles these charging rule report and take appropriate actions based on configuration done through **failure-policy** keyword.
Charging Rule Report comes through CCA or RAA messages in a call flow used for handling the charging-rule-report.
IPCF supports following charging rule failure codes in report:

- Out-of-credit
- Reallocation-of-credit
- Unknown rule name
- Invalid Rating Group
- Invalid Service Identifier
- GW/PCEF Malfunction
- Limited Resources
- Max No. of Bearers Reached
- Unknown Bearer Id
- Missing Bearer Id
- Missing Flow Description
- Resource Allocation Failure
- QoS Validation Failure

Charging rule status can any one of the following in this scenario:

- Active
- Inactive
- Temporarily Inactive

A charging rule report can occur in CCR message multiple times and maximum of 16 charging rule reports per CCR message is supported by IPCF.

Example

The following command sets the action for PCC-Data-Service named *temp_data1* for Dynamic Rule install with PCC-QoS-Profile named *temp_qos1* having precedence *22* and Gate-status as **Enabled** under PCC-Action-Set configuration instance for PCC-Service configuration:

```
dynamic-rule-install data-service temp_data1 qos-profile temp_qos1
precedence 22
```

dynamic-rule-uninstall

This command sets an action to uninstall a Dynamic Rule for the specified PCC-Data-Service in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] dynamic-rule-uninstall data-service data_svc_name [defer-by interval delayed_dur]
```

no

Removes the Dynamic Rule Uninstall action configured for specific PCC-Data-Service from a PCC-Action-Set configuration instance for PCC-Service configuration.

data-service *data_svc_name*

Specifies the name of the pre-configured PCC-Data-Service for which Dynamic Rules to be uninstalled under PCC-Action-Set configuration instance for PCC-Service configuration.
data_svc_name is a pre-configured PCC-Data-Service instance in PCC-Service Configuration mode.

defer-by interval *delayed_dur*

This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for dynamic rule removal.
delayed_dur configures the relative delay time by which the corresponding dynamic rule uninstallation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed.
delayed_dur specifies the delayed interval in *HH MIN SS* format.
Following format is used for *HH MIN SS* in *delayed_dur*:

- *HH* specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- *MIN* specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
- *SS* specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

Usage

Use this command to set an action to uninstall a PCC Dynamic rule for the specified PCC-Data-Service in PCC-Action-Set configuration for PCC-Service instance
Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding dynamic rule uninstallation is deferred.

Example

The following command sets the action of Dynamic Rule uninstall for PCC-Data-Service named *temp_data1* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
dynamic-rule-uninstall data-service temp_data1
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

log-event

This command allows operator to specify a string to be logged at Subscriber Service Controller (SSC) when the corresponding action set is triggered under PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] log-event msg-text message_string
```

no

Removes the notification message configured for specific action under a PCC-Action-Set configuration instance for PCC-Service configuration.

msg-text *message_string*

Specifies the message notification text string to be logged at the SSC when a particular PCC-Action-Set triggered for PCC-Service instance.
message_string is a string of alphanumerical characters of 1 through 255 characters

Usage

Use this command to allow operator to specify a string to be logged at Subscriber Service Controller (SSC) when the corresponding action set is triggered under PCC-Action-Set configuration for PCC-Service instance.

Example

The following command sets the notification message for an action under PCC-Action-Set configuration instance for PCC-Service configuration:

```
log-event msg-text "This Action is Applicable for EPS Session Only."
```

notify-user

This command allows operator to specify a string template-id at SSC under PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] notify-user message-id message_id [parameter value_pair]
```

no

Removes the user notification message id configured for specific action under a PCC-Action-Set configuration instance for PCC-Service configuration.

message-id *message_id*

Specifies the message template id stored at SSC to be used for user notification for action under PCC-Action-Set configuration for PCC-Service instance.
message_id is a string of alphanumerical characters of 1 through 255 characters

parameter *value_pair*

Specifies the parameters in the form of name value pairs separated by comma. A maximum of 16 name value pairs can be defined for action under PCC-Action-Set configuration for PCC-Service instance.
The name value pairs is encoded into **xml** data like other parameters and sent out to SSC for user notification.
value_pair is a string of alphanumerical characters of 1 through 255 characters which can accommodate up to 16 name value pair separated by comma (,).

Usage

Use this command to allow operator to specify a string template-id under PCC-Action-Set configuration for PCC-Service instance.
The template description exists at SSC and when the corresponding action set is hit, the subscriber is notified with the specified template configured via this command.
The action set makes a XML remote procedure call towards SSC. The XML contains information like IMSI, template-id of the SMS/E-mail template and other details like MSISDN, NAI if available. To give more flexibility to the operator, now the this command accepts name value pairs, which are also sent along with the said data.

Example

The following command sets the message id *"Invalid User."* for user notification message to an action under PCC-Action-Set configuration instance for PCC-Service configuration:

```
notify-user message-id "Invalid User."
```

offline-charging-server

This command sets the action to change the offline charging server applicable to an IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

[no] offline-charging-server primary *pri_serv_address* [**secondary** *sec_serv_address*]

no

Removes the action set to change the offline charging server under PCC-Action-Set configuration instance for PCC-Service configuration.

primary *pri_serv_address*

Identifies the name of the primary offline charging server which is to be used for action to change under PCC-Action-Set configuration instance for PCC-Service configuration.
The *pri_serv_address* must be the address of an offline charging server in Diameter URI format (*FQDN* [*port*] [*transport*] [*protocol*]).

secondary *sec_serv_address*

Identifies the name of the secondary offline charging server which is to be used for action to change under PCC-Action-Set configuration instance for PCC-Service configuration.
The *sec_serv_address* must be the address of an offline charging server in Diameter URI format (*FQDN* [*port*] [*transport*] [*protocol*]).

Usage

Use this command to set an action to change the offline charging server applicable to an IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

Example

Following command configures an action change the offline charging server to primary server *aaa://host.abc.com:6666;transport=tcp;protocol=diameter* and secondary server *aaa://host.xyz.com:6666;transport=sctp;protocol=radius* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
offline-charging-server primary
aaa://host.abc.com:6666;transport=tcp;protocol=diameter secondary
aaa://host.xyz.com:6666;transport=sctp;protocol=radius
```

online-charging-server

This command sets the action to change the online charging server applicable to an IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

[**no**] **online-charging-server primary** *pri_serv_address* [**secondary** *sec_serv_address*]

no

Removes the action set to change the online charging server under PCC-Action-Set configuration instance for PCC-Service configuration.

primary *pri_serv_address*

Identifies the name of the primary online charging server which is to be used for action to change under PCC-Action-Set configuration instance for PCC-Service configuration.
The *pri_serv_address* must be the address of an online charging server in Diameter URI format (*FQDN* [*port*] [*transport*] [*protocol*]).

secondary *sec_serv_address*

Identifies the name of the secondary online charging server which is to be used for action to change under PCC-Action-Set configuration instance for PCC-Service configuration.
The *sec_serv_address* must be the address of an online charging server in Diameter URI format (*FQDN* [*port*] [*transport*] [*protocol*]).

Usage

Use this command to set an action to change the online charging server applicable to an IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

Example

Following command configures an action change the online charging server to primary server *aaa://host.abc.com:6666;transport=tcp;protocol=diameter* and secondary server *aaa://host.xyz.com:6666;transport=sctp;protocol=radius* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
online-charging-server primary
aaa://host.abc.com:6666;transport=tcp;protocol=diameter secondary
aaa://host.xyz.com:6666;transport=sctp;protocol=radius
```

request-usage-report monitoring-key

This command configures the action to allow operator to explicitly request usage report for the specified Monitoring Key or all Monitoring Keys under PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] request-usage-report monitoring-key {mon_key_id | any}
```

no

Removes the usage request action configuration for Monitoring Key id from a PCC-Action-Set configuration instance for PCC-Service configuration.

mon_key_id

Specifies the Monitoring Key identifier for which usage report action is to be set under PCC-Action-Set configuration instance for PCC-Service configuration.
mon_key_id must be an integer between 1 through 65535.

any

Specifies the Monitoring Key identifier to "ANY" value for which usage report action is to be set under PCC-Action-Set configuration instance for PCC-Service configuration.

Usage

Use this command to configure the action to allow operator to explicitly request usage report for the specified Monitoring Key or all Monitoring Keys under PCC-Action-Set configuration for PCC-Service instance.

Example

The following command sets an action to request the usage report for Monitoring Key id *102* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
request-usage-report monitoring-key 102
```

rule-activate

This command sets an action to activate a pre-configured Rule in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] rule-activate rule_name[defer-by interval delayed_dur]
```

no

Removes the action to activate a pre-configured Rule from a PCC-Action-Set configuration instance for PCC-Service configuration.

rule_name

Specifies the name of the pre-configured Rule on PCEF for an activation action is set under PCC-Action-Set configuration instance for PCC-Service configuration.
rule_name is a pre-configured Rule in PCEF.

defer-by interval *delayed_dur*

This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for rule activation.
delayed_dur configures the relative delay time by which the corresponding rule activation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed.
delayed_dur specifies the delayed interval in *HH MIN SS* format.
Following format is used for *HH MIN SS* in *delayed_dur*:

- *HH* specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- *MIN* specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
- *SS* specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

Usage

Use this command to set an action to activate a pre-configured Rule in PCC-Action-Set configuration for PCC-Service instance.
Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding rule activation is deferred.

Example

The following command sets an action to activate for Rule *rule1* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
rule-activate rule1
```

rule-deactivate

This command sets an action to deactivate a pre-configured Rule in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] rule-deactivate rule_name [defer-by interval delayed_dur]
```

no

Removes the action to deactivate a pre-configured Rule from a PCC-Action-Set configuration instance for PCC-Service configuration.

rule_name

Specifies the name of the pre-configured Rule on PCEF for a deactivation action is set under PCC-Action-Set configuration instance for PCC-Service configuration.
rule_name is a pre-configured Rule in PCEF.

defer-by interval *delayed_dur*

This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for rule deactivation.
delayed_dur configures the relative delay time by which the corresponding rule deactivation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed.
delayed_dur specifies the delayed interval in *HH MIN SS* format.
Following format is used for *HH MIN SS* in *delayed_dur*:

- *HH* specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- *MIN* specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
- *SS* specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

Usage

Use this command to set an action to deactivate a pre-configured Rule in PCC-Action-Set configuration for PCC-Service instance.
Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding rule deactivation is deferred.

Example

The following command sets an action to deactivate for Rule *rule1* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
rule-deactivate rule1
```

rulebase-activate

This command sets an action to activate a pre-configured Rulebase in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] rulebase-activate rulebase_name [defer-by interval delayed_dur]
```

no

Removes the action to activate a pre-configured Rulebase from a PCC-Action-Set configuration instance for PCC-Service configuration.

rulebase_name

Specifies the name of the pre-configured Rulebase on PCEF for an activation action is set under PCC-Action-Set configuration instance for PCC-Service configuration.
rulebase_name is a pre-configured Rulebase in PCEF.

defer-by interval *delayed_dur*

This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for Rulebase activation.
delayed_dur configures the relative delay time by which the corresponding Rulebase activation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed.
delayed_dur specifies the delayed interval in *HH MIN SS* format.
Following format is used for *HH MIN SS* in *delayed_dur*:

- *HH* specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- *MIN* specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
- *SS* specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

Usage

Use this command to set an action to activate a pre-configured Rulebase in PCC-Action-Set configuration for PCC-Service instance.
Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding Rulebase activation is deferred.

Example

The following command sets an action to activate for Rulebase *rulebase1* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
rulebase-activate rulebase1
```

rulebase-deactivate

This command sets an action to deactivate a pre-configured Rulebase in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

[no] rulebase-deactivate *rulebase_name* [**defer-by interval** *delayed_dur*]

no

Removes the action to deactivate a pre-configured Rulebase from a PCC-Action-Set configuration instance for PCC-Service configuration.

rulebase_name

Specifies the name of the pre-configured Rulebase on PCEF for a deactivation action is set under PCC-Action-Set configuration instance for PCC-Service configuration.
rule_name is a pre-configured Rulebase in PCEF.

defer-by interval *delayed_dur*

This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for Rulebase deactivation.
delayed_dur configures the relative delay time by which the corresponding Rulebase deactivation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed.
delayed_dur specifies the delayed interval in *HH MIN SS* format.
Following format is used for *HH MIN SS* in *delayed_dur*:

- *HH* specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- *MIN* specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
- *SS* specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

Usage

Use this command to set an action to deactivate a pre-configured Rulebase in PCC-Action-Set configuration for PCC-Service instance.
Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding Rulebase deactivation is deferred.

Example

The following command sets an action to deactivate for Rulebase *rulebase1* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
rulebase-deactivate rulebase1
```

service-tag

This command sets an action to activate/deactivate a pre-configured Service Tag rule in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] service-tag svc_tag {activate-rule | activate-rule}
```

no

Removes the action to activate/deactivate a pre-configured Service Tag rule in PCC-Action-Set configuration for PCC-Service instance.

svc_tag

Specifies the name of the pre-configured Service Tag rule for an activation/deactivation is set under PCC-Action-Set configuration instance for PCC-Service configuration.
svc_tag is a pre-configured Service Tag name.

activate-rule

Specifies that action to be set for Service Tag activation rule under PCC-Action-Set configuration instance for PCC-Service configuration.

deactivate-rule

Specifies that action to be set for Service Tag deactivation rule under PCC-Action-Set configuration instance for PCC-Service configuration.

Usage

Use this command to set an action to activate/deactivate a pre-configured Service Tag rule in PCC-Action-Set configuration for PCC-Service instance.

Example

The following command sets the an activation rule for Service Tag named *service_1* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
service-tag service_1 activate-rule
```

terminate-session

This command sets an action to terminate a Bearer based on **bearer-id** or unique combination of QCI and ARP received through current CCR message in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] terminate-session
```

no

Removes the action to terminate a Bearer based on **bearer-id** from a PCC-Action-Set configuration instance for PCC-Service configuration.

Usage

Use this command to set an action to terminate a Bearer based on **bearer-id** or unique combination of QCI and ARP received through current CCR message in PCC-Action-Set configuration for PCC-Service instance. Termination of Bearer is possible only in case of PCRF binding and limited to Dynamic rules.

Important: This action is only applicable to IP-CAN sessions with access type as GPRS. When terminate Bearer is initiated, IPCF triggers **Bearer Termination Procedure** for the **bearer-id** received through current CCR message.

Caution: This command triggers termination of **Gx** and SPR sub session active under PCC-Service instance.

Example

The following command sets an action to terminate a Bearer based on **bearer-id** received through current CCR message under PCC-Action-Set configuration instance for PCC-Service configuration:

```
terminate-session
```

usage-monitor

This command sets an action to allow operator to stop, reset or start the counting for a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] usage-monitor usage_mon_name {reset-counter | start-counter | stop-counter}
```

no

Removes the action to allow operator to stop, reset or start the counting for a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

usage_mon_name

Specifies the name of the pre-configured PCC-Usage-Monitor for which counter action is configured under PCC-Action-Set configuration instance for PCC-Service configuration.
usage_mon_name is a pre-configured PCC-Usage-Monitor.

reset-counter

Resets the usage counts for PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.

start-counter

Starts the accumulation of usage counts for PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.

stop-counter

Stops the accumulation of usage counts for PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.

Usage

Use this command to set an action to allow operator to stop, reset or start the counting for a usage monitor in PCC-Action-Set configuration for PCC-Service instance.

Example

The following command sets the an action to stop the accumulation of usage counts for PCC-Usage-Monitor named *usage_1* under PCC-Action-Set configuration instance for PCC-Service configuration:

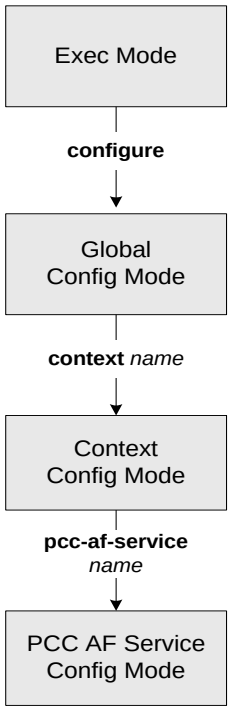
```
usage-monitor usage_1 stop-counter
```

Chapter 216
PCC-AF-Service Configuration Mode Commands

The PCC-AF-Service Configuration mode provides a mechanism to IPCF to manage the external interfaces required for media and application function management. The PCC-AF-Service manages **Rx** interface which would be based on the dictionary used.

An Application Function (AF) provides Application (layer 7) proxies for client server applications. It also provides enforcement of operator and subscriber QoS, Charging, and Security policies to subscriber session and represents the network element that supports applications that require dynamic policy and/or charging control. In the IMS model, the AF is implemented by the Proxy Call Session Control Function (P-CSCF).

Important: This configuration mode is supported from StarOS Release 12.1 onward.



associate pcc-service

This command is used to associate a pre-configured PCC-Service with a PCC-AF-Service for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

associate pcc-service *pcc_svc_name*

[**no**] **associate pcc-service**

no

Removes/disassociate the configured PCC-service from this PCC-AF-Service instance configured for IPCF configuration.

pcc_svc_name

Specifies the name of a pre-configured PCC-service configured in Context Configuration mode for IPCF configuration.
The *pcc_svc_name* is name of a predefined PCC-Service instance and must be an alphanumerical string from 1 through 63 characters.

Usage

Use this command to associate a pre-configured PCC-Service instance for IPCF configuration.

Important: For more information on PCC-Service configuration, refer *PCC-Service Configuration Mode Commands*.

Example

Following command binds a PCC-Service named *pcc_svc1* with in a PCC-AF-Service.

```
associate pcc-service pcc_svc1
```

Following command removes an associated PCC-Service named *pcc_svc1* from a PCC-AF-Service.

```
no associate pcc-service pcc_svc1
```

diameter dictionary

This command is used to assign a Diameter dictionary for **Rx** messaging with a PCC-AF-Service for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

diameter dictionary {**r8-standard** | **standard**}

default diameter dictionary

default

Sets the Diameter **Rx** dictionary to default dictionary **r8-standard** (3GPP Rel. 8 standard) for a PCC-AF-Service instance configured for IPCF configuration.

r8-standard

Default: Enabled
Sets the Diameter **Rx** dictionary to be used by a PCC-AF-Service instance configured for IPCF configuration over **Rx** interface to 3GPP Rel. 8 standard.

standard

Default: Disabled
Sets the Diameter **Rx** dictionary to be used by a PCC-AF-Service instance configured for IPCF configuration over **Rx** interface to 3GPP Rel. 7 standard.

Usage

Use this command to configure the PCC-AF-Service to determine which of the 3GPP dictionary to be used for **Rx** interface messaging for media and application function management.

Example

Following command sets the PCC-AF-Service to use 3GPP Rel. 8 standard dictionary for **Rx** interface and application function management related messaging in a PCC-AF-Service.

```
default diameter dictionary
```

diameter origin end-point

This command is used to bind/associate a pre-configured Diameter host/realm (AF) over **Rx** interface with a PCC-AF-Service to be used for subscriber service control and AF profile management.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

diameter origin endpoint *dia_endpoint_name*

no diameter origin endpoint

no

Removes the associated Diameter Origin Endpoint configuration from PCC-AF-Service instance configured for IPCF configuration.

any

Sets the PCC-AF-Service instance to use any available AF node over **Rx** interface for AF support.

dia_endpoint_name

The *dia_endpoint_name* is a predefined Diameter origin endpoint node and must be an alphanumerical string from 1 through 63 characters.

Usage

Use this command to bind the AF node over **Rx** interface by associating a pre-configured Diameter Origin Endpoint with a PCC-AF-Service.
The Diameter origin endpoint must be a pre-configured instance in the Context Configuration Mode. For more information on Diameter origin endpoint configuration, refer *Diameter Endpoint Configuration Mode Commands* chapter.

Example

Following command associates a pre-configured Diameter endpoint node configuration named *af_pcscf1* with a PCC-AF-Service for AF profile management.

```
diameter origin endpoint af_pcscf1
```

Following command removes the pre-associated Diameter endpoint node configuration named *af_pcscf1* with a PCC-AF-Service.

```
no diameter origin endpoint
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

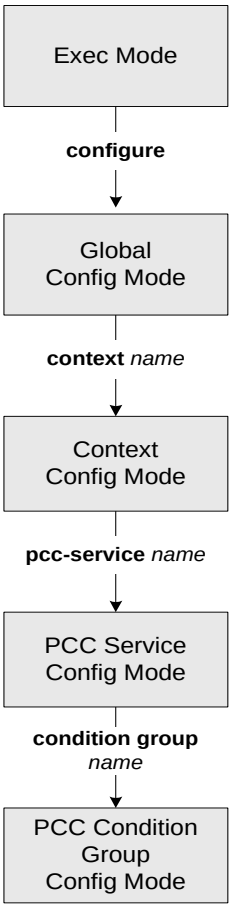
Usage

Use this command to return to the parent configuration mode.

Chapter 217
PCC-Condition-Group Configuration Mode Commands

The PCC-Condition-Group Configuration Mode is used to configure the various rating parameters under a logical identifier name in the PCC-Service. A PCC-Condition-Group is a collection of conditions that identify a network or state constraint represented as a logical expression. A maximum of 128 conditions can be configured in one PCC-Condition-Group.

Important: This configuration mode is supported from StarOS Release 12.1 onward.



af-application-id

This command defines a condition based on the application id of an Application Function service through the **Rx** interface over which the IPCF receives media information for the application usage in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] af-application-id operator af_app_id
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the AF-Application id.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

af_app_id

Specifies the identity string for AF-Application identifier over **Rx** interface.
af_app_id must be an alphanumeric string of 1 to 256 characters.

Usage

Use this command to define a condition based on the application id of an Application Function service through the **Rx** interface over which the IPCF receives media information for the application usage in an IP-CAN session.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the AF Application id is not equal to *pcc_af_1*:

```
af-application-id != pcc_af_1
```

af-media-codec

This command defines a condition based on the media Codec used by AF application in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] af-media-coded *operator* {**g722** | **g726** | **ilbc** | **pcma** | **pcmu**}

no

Removes the specified condition definition.

operator

Specifies how to logically match the AF-media Codec.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

g722

Specifies the media Codec as G.722 used for user traffic from AF server over **Rx** interface.
G.722 is a ITU-T standard 7 kHz wideband speech codec operating at 48, 56 and 64 kbit/s.

g726

Specifies the media codec as G.726 used for user traffic from AF server over **Rx** interface.
G.726 is an ITU-T ADPCM speech codec standard covering the transmission of voice at rates of 16, 24, 32, and 40 kbit/s.

ilbc

Specifies the media codec as Internet Low Bitrate Codec (iLBC) used for user traffic from AF server over **Rx** interface.
iLBC is a narrowband speech codec suitable for VoIP applications, streaming audio, archival and messaging. The encoded blocks encapsulated in Real-time Transport Protocol (RTP) protocol for transport.

pcma

Specifies the media codec as Pulse Code Modulation A-law scaling (PCMA) used for user traffic from AF server over **Rx** interface.
PCMA is an ITU-T Recommendation G.711 audio data encoding in eight bits per sample, after A-law logarithmic scaling.

pcmu

Specifies the media codec as Pulse Code Modulation mu-law scaling (PCMU) used for user traffic from AF server over **Rx** interface.

PCMU is an ITU-T Recommendation G.711 audio data encoding in eight bits per sample, after mu-law logarithmic scaling.

Usage

Use this command to define a condition based on the media codecs used by AF service through the **Rx** interface over which the IPCF receives media information for the application usage in an IP-CAN session.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the AF Media codec is equal to PCMA:

```
af-media-codec = pcma
```

af-media-type

This command defines a condition based on the media type used by AF application in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] af-media-type *operator* {**application** | **audio** | **control** | **data** | **message** | **other** | **text** | **video**}

no

Removes the specified condition definition.

operator

Specifies how to logically match the media type in user traffic.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

application

Specifies the media type as Application in user traffic from AF server over **Rx** interface.

audio

Specifies the media type as Audio in user traffic from AF server over **Rx** interface.

control

Specifies the media type as Control in user traffic from AF server over **Rx** interface.

data

Specifies the media type as Data in user traffic from AF server over **Rx** interface.

message

Specifies the media type as Message in user traffic from AF server over **Rx** interface.

text

Specifies the media type as Text in user traffic from AF server over **Rx** interface.

video

Specifies the media type as Video in user traffic from AF server over **Rx** interface.

Usage

Use this command to define a condition based on the media type used by AF service through the **Rx** interface over which the IPCF receives media information for the application usage in an IP-CAN session.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the AF Media type is equal to Video:

```
af-media-type = video
```

af-service-urn

This command defines a condition based on the service Uniform Resource Names (URNs) used by AF application in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] af-service-urn *operator urn_string*

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

urn_string

Specifies the URN in user traffic from AF server over **Rx** interface.
urn_string must be an alphanumeric string of 1 through 256 characters.

Usage

Use this command to define a condition based on the URN used by AF service through the **Rx** interface over which the IPCF receives media information for the application usage in an IP-CAN session.
Uniform Resource Names (URNs) serves as persistent, location-independent resource identifiers and are designed to make it easy to map other namespaces into URN-space.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the AF service URN is equal to *ietf:rfc:4003*:

af-service-urn = *ietf:rfc:4003*

an-gw-address

This command defines a condition based on the IP address of Access Node Gateway (AN-GW) on which subscriber is attached in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] an-gw-address {*operator angw_ip/mask* | {**in-range** | **!in-range**} *range_start_ip* **to** *range_end_ip*}

---

no

Removes the specified condition definition.

---

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

---

in-range

Specifies the condition to accept the IP address which are in range as argument to define the Access Node Gateway address which is used by subscriber in IP-CAN session.

!in-range

Specifies the condition to accept the IP address which are NOT in range as argument to define the Access Node Gateway address which is used by subscriber in IP-CAN session.

---

range_start_ip

Specifies the starting IP address which is used for defining the range of AN-GW IP addresses which is used by subscriber in IP-CAN session.
range_start_ip is an IP address and must be lesser than *end_start_ip* address.

---

range_end_ip

Specifies the ending IP address which is used for defining the range of AN-GW IP addresses which is used by subscriber in IP-CAN session.
range_end_ip is an IP address and must be greater than *end_start_ip* address.

---

angw_ip/mask

Specifies the IP address of the Access Node Gateway which is used by subscriber in IP-CAN session along with IP mask as well.
angw_ip must be an IP address in IPv4 or IPv6 notation.

mask Specifies the IP address mask bits to determine the number of IP addresses of AN-GW in condition. *mask* must be specified using the standard IPv4 dotted decimal notation.

Usage

Use this command to define a condition based on the AN-GW IP address used by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on AN-GW IP address *1.2.3.4* in an IP-CAN session:

```
an-gw-address = 1.2.3.4
```

authorized-qci

This command defines a condition based on the authorized QoS Class Identifier used in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] authorized-qci operator qci
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

qci

Specifies the authorized QoS class identifier in user traffic for condition validation.
qci must be an integer between 1 through 255.

Usage

Use this command to define a condition based on the authorized QCI used by the subscriber in an IP-CAN session.
The condition evaluates to TRUE, if Bearer Control Mode is UE and network (PCEF bearer binding) and IPCF has authorized the specified QCI earlier.
QCI is a number which describes the error rate and delay that are associated with the service. It includes bearer parameters including scheduling weights and queue management thresholds.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the authorized QCI is greater than or equal to *4*:

```
authorized-qci >= 4
```

base-station-id

This command defines a condition based on the various parameters used in base-station id by subscriber in an IP-CAN session between PCEF (PDSN) and IPCF over **Gx** interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] base-station-id {[sid operator sys_identifier] | range start_range to end_range]]
[nid operator netwrk_identifier ] | range start_range to end_range ]] [ cellid operator
cell_identifier ] | range start_range to end_range ]]}
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **<**: Lesser than
- **<=**: Lesser than or equals
- **=**: Equals
- **>**: Greater than
- **>=**: Greater than or equals

sid *operator sys_identifier*

Specifies the system identifier in base-station id of subscriber for condition validation in an IP-CAN session.
sys_identifier must be an integer between 0 through 65535.

nid *operator netwrk_identifier*

Specifies the network identifier in base-station id, which is used by subscriber, for condition validation in an IP-CAN session.
netwrk_identifier must be an integer between 0 through 65535.

cellid *operator cell_identifier*

Specifies the cell identifier in base-station id, which is used by subscriber, for condition validation in an IP-CAN session.
cell_identifier must be an integer between 0 through 65535.

range *start_range* **to** *end_range*

This optional keyword specifies range of the identifiers (SID, Cell id, Network Id) to be used for condition validation in an IP-CAN session.

start_range is the start value of range having integer between 0 through 65535 and it must be lesser than *end_range*.
end_range is the end value of range having integer between 0 through 65535 and it must be greater than *start_range*.

Usage

User this command to define a condition based on the parameters used in base-station id of subscriber, which is composition of SID, Cell Id, and/or Network Id, in an IP-CAN session between PCEF (PDSN) and IPCF over **Gx** interface.
This condition is defined for PCC functionality support to CDMA users over **Gx** interface.

Example

The following command creates a condition definition to analyze the condition based on base-station id of subscriber where SID is *1001* and cell id is in range of *2001* to *2069* in an IP-CAN session between PDSN and IPCF having network id as *3989*:

```
base-station-id sid = 1001 nid = 3989 cellid = range 2001 to 2069
```

bearer-count

This command defines a condition based on the number of bearers allowed in a subscriber session on IPCF to accept bearer-count in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] bearer-count *operator num_bearer*

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

num_bearer

Specifies the number of bearers in user traffic for condition validation.
num_bearer indicates a condition based on the number of bearer established in a IP-CAN session and must be an integer between 1 through 11.

Usage

Use this command to define a condition based on the number of bearers allowed for a subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the PCC service user traffic for bearers allowed in a subscriber session is equal to *4*:

```
bearer-count = 4
```

connectivity-access-network

This command defines a condition based on the access network type used by subscriber in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] connectivity-access-network operator {3gpp-gprs | 3gpp2 | 3gpp2-eps | docsis | wimax | xdsl}
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the media type in user traffic.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

3gpp-gprs

Specifies the network access connectivity type as 3GPP-GPRS for user traffic in condition definition.

3gpp2

Specifies the network access connectivity type as 3GPP2 (CDMA) for user traffic in condition definition.

3gpp2-eps

Specifies the network access connectivity type as 3GPP2-EPS for user traffic in condition definition.

docsis

Specifies the network access connectivity type as Data Over Cable Service Interface Specification (DOCSIS) for user traffic in condition definition.

wimax

Specifies the network access connectivity type as Wi-MAX for user traffic in condition definition.

xdsl

Specifies the network access connectivity type as xDSL (ADSL/SDSL) or user traffic in condition definition.

Usage

Use this command to define a condition based on the type of connectivity used for network access by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the network type is equal to Wi-MAX:

```
connectivity-access-network = wimax
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

eval-condition-group

Defines a condition based on the TRUE or FALSE setting of a configured PCC-Condition-Group for subscriber in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] eval-condition-group *cond_grp_name operator* **{ FALSE | TRUE }**

no

Removes the specified condition definition.

cond_grp_name

Specifies the name of the configured PCC-Condition-Group which is used for evaluation with in this PCC-Condition-Group for user traffic.

operator

Specifies how to logically match the media type in user traffic.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

FALSE

Sets the evaluation condition for specified PCC-Condition-Group to FALSE.
With this keyword system rejects all conditions defined in specific PCC-Condition-Group and match the same in user traffic.

TRUE

Sets the evaluation condition for specified PCC-Condition-Group to TRUE.
With this keyword system accepts all conditions defined in specific PCC-Condition-Group and match the same in user traffic.

Usage

Use this command to define a condition based on the acceptance or rejection of specific pre-configured PCC-Condition-Group for user traffic in an IP-CAN session.
This command allows the operator to use configured PCC-Condition-Group in another PCC-Condition-Group as subset of PCC-Condition-Group.

Important: A maximum of 3 level of recursion depth is allowed for PCC-Condition-Group evaluation in a PCC-Condition-Group.

Example

The following command creates a condition definition to accept the all conditions defined in PCC-Condition-Group named *af_1*:

```
eval-condition-group af_1 = TRUE
```

eval-condition-group

This command defines a condition based on the TRUE or FALSE setting of a configured PCC-Condition-Group for subscriber in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] eval-condition-group cond_grp_name operator {FALSE | TRUE}
```

no

Removes the specified condition definition.

cond_grp_name

Specifies the name of the configured PCC-Condition-Group which is used for evaluation with in this PCC-Condition-Group for user traffic.
cond_grp_name must be a pre-configured PCC-Condition-Group in this configuration mode.

operator

Specifies how to logically match the media type in user traffic.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

FALSE

Sets the evaluation condition for specified PCC-Condition-Group to FALSE.
With this keyword system rejects all conditions defined in specific PCC-Condition-Group and match the same in user traffic.

TRUE

Sets the evaluation condition for specified PCC-Condition-Group to TRUE.
With this keyword system accepts all conditions defined in specific PCC-Condition-Group and match the same in user traffic.

Usage

Use this command to define a condition based on the acceptance or rejection of specific pre-configured PCC-Condition-Group for user traffic in an IP-CAN session.
This command allows the operator to use configured PCC-Condition-Group in another PCC-Condition-Group as subset of PCC-Condition-Group.

Important: A maximum of 3 level of recursion depth is allowed for PCC-Condition-Group evaluation in a PCC-Condition-Group.

Example

The following command creates a condition definition to accept the all conditions defined in PCC-Condition-Group named *af_1*:

```
eval-condition-group af_1 = TRUE
```

event-time

This command defines a condition based on the event-trigger time as per the time specified by the named Time definition (Timedef) configured for subscriber session in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] event-time *operator timedef_name*

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

timedef_name

Specifies the name of the configured time definition (start and end timer of session) which is used for evaluation with this PCC-Condition-Group for user traffic.
timedef_name must be a pre-configured Time definition in *PCC-Service Configuration Mode*.

Usage

Use this command to define a condition based on the start and end time defined in a Time Definition configuration in *PCC-Service Configuration Mode* for user traffic in an IP-CAN session.
Event trigger in this command indicates a condition when the event-trigger time was as per the time specified by the named Time Definition.
This command allows the operator to use configured time period as event trigger for this PCC-Condition-Group.

Example

The following command creates a condition definition to trigger the condition based on the start and end time defined in Timedef named *timedef_night*:

```
event-time = timedef_night
```

event-trigger

This command defines a condition based on the event triggers due to various conditions for subscriber in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] event-trigger *operator event_trigger*

no

Removes the specified condition definition.

operator

Specifies how to logically match the media type in user traffic.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

event_trigger

Specifies the network events as condition definition for user traffic in an IP-CAN session.
Following event triggers are supported with this command:

- **an-gw-change**
- **bearer-qos-change**
- **bearer-setup**
- **bearer-termination**
- **default-eps-bearer-qos-change**
- **ip-can-change**
- **loss-of-bearer**
- **out-of-credit**
- **pgw-trace-control**
- **plmn-change**
- **qos-change**
- **qos-change-exceeding-authorization**
- **rai-change**
- **rat-change**
- **reallocation-of-credit**

- **recover-of-bearer**
- **resource-modification-request**
- **revalidation-timeout**
- **session-setup**
- **session-termination**
- **sgsn-change**
- **successful-resource-allocation**
- **tft-change**
- **ue-ip-address-allocate**
- **ue-ip-address-release**
- **ue-time-zone-change**
- **user-location-change**

Usage

Use this command to define a condition based on the event triggered in network for user traffic.

Example

The following command creates a condition definition when there is a change in traffic flow template for subscriber:

```
event-trigger = tft-change
```

imsi

This command defines a condition based on the International Mobile Station Identification number (IMSI) of a subscriber in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] imsi operator imsi
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

imsi

Specifies the IMSI of subscriber to be used for condition validation in an IP-CAN session.
imsi must be a string of between 8 to 15 digits which starts with 3 digit of MCC then 2 to 3 digit of MNC. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘). For example; ‘$’.

Usage

Use this command to define a condition based on the IMSI of a subscriber used in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on subscriber IMSI as *12334566434* in an IP-CAN session:

```
imsi = 12334566434
```

msisdn

This command defines a condition based on the Mobile Station International Subscriber Directory Number (MSISDN) of a subscriber in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] msisdn operator msisdn
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

imsi

Specifies the MSISDN of subscriber to be used for condition validation in an IP-CAN session.
msisdn must be a string of between 1 to 16 digits which contains CC + NDC/NPA + SN.
Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘). For example; ‘$’.

Usage

Use this command to define a condition based on the MS ISDN of a subscriber used in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on subscriber MSISDN as *380561234567* in an IP-CAN session:

```
msisdn = 380561234567
```

multi-line-or

This command enables/disables the “OR” relation across all conditions exist in PCC-Condition-Group Configuration Mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] multi-line-or
```

no

Sets the PCC-Condition-Group to “AND” relation across all conditions exist in a PCC-Condition-Group Configuration Mode.

Usage

Use this command to enable the “OR” relation across all conditions exist in PCC-Condition-Group Configuration Mode.
In absence of this command the default relation of “AND” applies across all conditions exist in PCC-Condition-Group Configuration Mode.

Example

The following command enables the “OR” relation across all conditions exist in *PCC-Condition-Group Configuration Mode*:

```
multi-line-or
```

The following command enables the default “AND” relation across all conditions exist in *PCC-Condition-Group Configuration Mode*:

```
no multi-line-or
```

nai

This command defines a condition based on the Network Access Identifier (NAI) of a subscriber in an IP-CAN session between PCEF (PDSN) and IPCF over **Gx** interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] nai operator {username user_name [domain domain] | domain domain}
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

username *user_name*

Specifies the subscriber user name to be used for condition validation in an IP-CAN session.
user_name must be an alpha and/or numeric string of 1 through 128 characters in length. The user name can contain all special characters.

domain *domain*

Specifies the domain (Realm) of subscriber to be used for condition validation in an IP-CAN session.
domain must be an alpha and/or numeric string of 1 through 128 characters in length. The domain name can contain all special characters.

Usage

User this command to define a condition based on the NAI, which contains of user name and domain name, of a subscriber in an IP-CAN session between PCEF (PDSN) and IPCF over **Gx** interface.
This condition is defined for PCC functionality support to CDMA users over **Gx** interface.

Example

The following command creates a condition definition to analyze the condition based on subscriber user name as *cdma2000_subs1* in an IP-CAN session between PDSN and IPCF having *xyz.com* as domain:

```
nai = username cdma2000_subs1 domain xyz.com
```

out-of-credit rulename

This command defines a condition based on the exhaustion of credit for subscriber Rulename at PCEF in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] out-of-credit rulename operator rule_name
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

rule_name

Specifies the name of the Rulename for which out of credit condition is to match in an IP-CAN session.
rule_name is a pre-configured Rulename on PCEF and must be an alphanumeric string of from 1 through 63 characters.

Usage

Use this command to define a condition based on the exhaustion of credit for subscriber Rulename at PCEF in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on the exhaustion of credit for subscriber Rulename *rule_101* at PCEF in an IP-CAN session:

```
out-of-credit rulename = rule_101
```

out-of-credit rulebase-name

This command defines a condition based on the exhaustion of credit for subscriber Rulebase name at PCEF in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] out-of-credit rulebase-name *operator rulebase_name*

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

rulebase_name

Specifies the name of the Rulebase for which out of credit condition is to match in an IP-CAN session. *rulebase_name* is a pre-configured Rulebase on PCEF and must be an alphanumeric string of from 1 through 63 characters.

Usage

Use this command to define a condition based on the exhaustion of credit for subscriber Rulebase name at PCEF in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on the exhaustion of credit for subscriber Rulebase name *rulebase_101* at PCEF in an IP-CAN session:

```
out-of-credit rulebase-name = rulebase_101
```

pcef-address

This command defines a condition based on the IP address of Policy and Charging Enforcement Function (PCEF) which is served by IPCF and through which subscriber is attached to an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[**no**] **pcef-address** {*operator pcef_ip/mask* | {**in-range** | **!in-range**} *range_start_ip* **to** *range_end_ip*}

---

no

Removes the specified condition definition.

---

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

---

in-range

Specifies the condition to accept the IP address which are in range as argument to define the PCEF address which is used by subscriber in IP-CAN session.

!in-range

Specifies the condition to accept the IP address which are NOT in range as argument to define the PCEF address which is used by subscriber in IP-CAN session.

---

range_start_ip

Specifies the starting IP address which is used for defining the range of PCEF IP addresses which is used by subscriber in IP-CAN session.
range_start_ip is an IP address and must be lesser than *end_start_ip* address.

---

range_end_ip

Specifies the ending IP address which is used for defining the range of PCEF IP addresses which is used by subscriber in IP-CAN session.
range_end_ip is an IP address and must be greater than *end_start_ip* address.

---

pcef_ip/mask

Specifies the IP address of the PCEF which is used by subscriber in IP-CAN session along with IP mask as well.
pcef_ip must be an IP address in IPv4 or IPv6 notation.

mask Specifies the IP address mask bits to determine the number of IP addresses of PCEF in condition. *mask* must be specified using the standard IPv4 dotted decimal notation.

Usage

Use this command to define a condition based on the PCEF IP address used by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on PCEF P address *1.2.3.4* in an IP-CAN session:

```
pcef-address = 1.2.3.4
```

pdn-id

This command defines a condition based on the PDN or calling station id in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] pdn-id [case-insensitive] *operator pdn_id*

no

Removes the specified condition definition.

case-insensitive

This optional keyword sets the condition to not to consider the case of argument phrase for condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals
- **contains**: Contains
- **!contains**: Does not contain
- **starts-with**: Starts with
- **!starts-with**: Does not start with
- **ends-with**: Ends with
- **!ends-with**: Does not end with

pdn_id

Specifies the PDN or calling station id to be used for condition validation in an IP-CAN session.
pdn_id must be an alphanumeric string of between 1 to 128 characters.

Usage

Use this command to define a condition based on the PDN or calling station id used in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on calling station id *ggsn_all_102* in an IP-CAN session:

pdn-id = *ggsn_all_102*

profile-attribute

This command defines a condition based on the matching between subscriber profile attribute value and SPR attribute value in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] profile-attribute parameter *subs_prof_attr_value operator spr_attr_value*

no

Removes the specified condition definition.

parameter *subs_prof_attr_value*

Specifies the attribute parameter value to match with SPR attribute for condition validation in an IP-CAN session.
subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

spr_attr_value

Specifies the attribute value in SPR to match with Subscriber profile attribute for condition validation in an IP-CAN session.
spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

Usage

Use this command to define a condition based on the matching parameters between subscriber profile attribute and SPR attribute parameters used in an IP-CAN session and provides a generic way of specifying and triggering actions based on any of the subscriber profile attribute received from SPR interactions.

Example

The following command creates a condition definition to analyze the condition based on matching of subscriber profile attribute value *subs_gold_102* with SPR attribute value *spr_gold_102*in an IP-CAN session:

```
profile-attribute parameter subs_gold_102 = spr_gold_102
```

radio-access-technology

This command defines a condition based on the radio access technology used by subscriber in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] radio-access-technology operator RAT
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the media type in user traffic.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

RAT

Specifies the radio access technology used by subscriber to access the network as condition definition for user traffic in an IP-CAN session.
Following RAT are supported with this command:

- **cdma2000-1x**: 3GPP2 CDMA 2000 - 1x RTT
- **eutran**: Evolved Universal Terrestrial Radio Access Network (eUTRAN)
- **gan**: Generic Access Network (GAN)
- **geran**: GSM Edge Radio Access Network (GERAN)
- **hrpd**: High Rate Packet Data (CDMA 2000 1xEV-DO)
- **hspa-evolution**: Evolved High-Speed Packet Access (eHSPA/HSPA+)
- **umb**: Ultra-Mobile Broadband
- **utran**: Universal Terrestrial Radio Access Network (UTRAN)
- **wlan**: Wireless Local Area Network (WLAN/xDSL)

Usage

Use this command to define a condition based on the type of radio technology used for network access by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the radio access technology type as WLAN:

```
radio-access-technology = wlan
```

sgsn-ip

This command defines a condition based on the IP address of SGSN on which subscriber is attached in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] sgsn-ip {operator sgsn_ip/mask | {in-range | !in-range} range_start_ip to
range_end_ip}
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

in-range

Specifies the condition to accept the IP address which are in range as argument to define the SGSN address which is used by subscriber in IP-CAN session.

!in-range

Specifies the condition to accept the IP address which are NOT in range as argument to define the SGSN address which is used by subscriber in IP-CAN session.

range_start_ip

Specifies the starting IP address which is used for defining the range of SGSN IP addresses which is used by subscriber in IP-CAN session.
range_start_ip is an IP address and must be lesser than *end_start_ip* address.

range_end_ip

Specifies the ending IP address which is used for defining the range of SGSN IP addresses which is used by subscriber in IP-CAN session.
range_end_ip is an IP address and must be greater than *end_start_ip* address.

sgsn_ip/mask

Specifies the IP address of the SGSN which is used by subscriber in IP-CAN session along with IP mask as well.
sgsn_ip must be an IP address in IPv4 or IPv6 notation.

mask Specifies the IP address mask bits to determine the number of IP addresses of SGSN in condition. *mask* must be specified using the standard IPv4 dotted decimal notation.

Usage

Use this command to define a condition based on the SGSN IP address used by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on SGSN IP address *1.2.3.4* in an IP-CAN session:

```
sgsn-ip = 1.2.3.4
```

sgsn-mcc-mnc

This command defines a condition based on the PLMN (MCC+MNC) of SGSN on which subscriber is attached in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] sgsn-mcc-mnc operator {mcc mcc_value [mnc mnc_value] | [mcc mcc_value] mnc
mnc_value}
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

mcc *mcc_value*

Specifies the Mobile Country Code in PLMN of SGSN which is used by subscriber in IP-CAN session.
mcc_value must be an integer between 101 and 998.

mnc *mnc_value*

Specifies the Mobile Network Code in PLMN of SGSN which is used by subscriber in IP-CAN session.
mnc_value must be an integer between 1 and 998.

Usage

Use this command to define a condition based on the PLMN of SGSN used by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on PLMN of SGSN with MCC as *102* and MNC as *99*in an IP-CAN session:

```
sgsn-mcc-mnc = mcc 102 mnc 99
```

subscription-attribute

This command defines a condition based on the matching between subscriber subscription attribute value and SPR attribute value in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] subscription-attribute *subsription_attr_value operator spr_attr_value*

no

Removes the specified condition definition.

subsription_attr_value

Specifies the subscriber subscription attribute value to match with SPR attribute for condition validation in an IP-CAN session.
subsription_attr_value must be an alphanumeric string of from 1 through 31 characters.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

spr_attr_value

Specifies the attribute value in SPR to match with subscriber subscription attribute for condition validation in an IP-CAN session.
spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

Usage

Use this command to define a condition based on the matching parameters between subscriber subscription attribute and SPR attribute value used in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on matching of subscriber subscription attribute value *subs_gold_102* with SPR attribute value *spr_gold_101*in an IP-CAN session:

subscription-attribute *subscribe_gold_102* **=** *spr_gold_101*

spr-profile-not-found

This command defines a condition based on the availability of SPR profile for s subscriber in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] spr-profile-not-found
```

no

Removes the specified condition definition.

Usage

Use this command to define a condition based on the availability of SPR profile for a subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition if SPR profile is not available for a subscriber in an IP-CAN session:

```
spr-profile-not-found
```

threshold-condition usage-monitor

This command defines a condition based on the threshold conditions in usage of traffic by subscriber session in an IP-CAN session. It is used to support usage tracking and dynamic Policy control based on subscriber usage.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] threshold-condition usage-monitor *usage_mon_name* **usage** *operator* {**absolute value** *volume* | **subscription-limit** | **subscription-threshold** *subs_thres_limit*}

no

Removes the specified condition definition.

usage_mon_name

Specifies a unique name for configured usage monitor condition which is used for evaluation with this condition group for user traffic in IP-CAN session.
usage_mon_name must be an alphanumeric string of 1 through 63 characters.

usage

This keyword specifies the condition as usage for threshold condition which is used for evaluation with this condition group for user traffic in IP-CAN session.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

absolute value *volume*

Specifies the threshold limit condition definition based on absolute usage volume *volume* in Kilo Bytes which is used for evaluation with this condition group for user traffic in IP-CAN session.
volume must be an integer between 1 through 4294967295.

subscription-limit

Specifies the threshold limit condition based on Subscriber's subscription limit which is used for evaluation with this condition group for user traffic in IP-CAN session.
In this condition the system takes Subscriber's subscription limit as defined in subscriber subscription policy for threshold limit monitoring.

subscription-threshold *subs_thres_limit*

Specifies the condition definition for threshold limit based on a configured usage monitor threshold named *subs_thres_limit* in IP-CAN session.
subs_thres_limit is a pre-configured subscription limit in this configuration mode.
This command allows the operator to use configured subscription limit as subset of a threshold condition.

Usage

Use this command to define a condition based on the duration of usage of service in seconds or volume usage in Bytes for user traffic in an IP-CAN session. This usage monitor is used to support usage tracking and dynamic Policy control based on subscriber usage.
IPCF supports the concept of Monitoring Key. PCEF, when instructed by PCRF, keeps track of usage per Monitoring Key. PCEF reports the usage when thresholds are reached or requested by PCRF.
To allow operator to have dynamic Policy control, IPCF uses Usage Monitor. This Usage Monitor has single attribute of volume-limit. Operator can "associate" different Monitoring Keys to these usage monitors. It can be a Many-To-Many relationship between Usage-Monitor and Monitoring-Key. Operator can use Usage conditions on Usage Monitors instead of Monitoring Keys directly.
IPCF tracks usage per usage-monitor. Different monitoring keys associated to a Usage-Monitor. When monitoring key is associated to a Usage-Monitor, the usage reported for that particular monitoring key is added to all the usage monitoring to which it is associated.
IPCF supports 2 types of usage monitors; it can be defined on IPCF or SSC supplied usage monitors. The name *usage_mon_name* identifies an usage-monitor, which is locally defined or received from SSC. The **absolute** value applies to both types of usage monitors.
This command allows the operator to use configured threshold condition with another threshold condition as subset.
A maximum of 8 thresholds can be configured per usage monitor.

Example

The following command creates a threshold condition with usage monitor name *threshold1* as usage monitor to trigger the condition based on the **subscription limit** as provide in Subscriber policy:

```
threshold-condition usage-monitor threshold1 usage = subscription-limit
```

user-access-network

This command defines a condition based on the access location type of the subscriber in an IP-CAN session as received on **Gx** interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] user-access-network operator {home | roaming | visiting}
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

home

Specifies the subscriber network access type as Home for condition validation in an IP-CAN session. This condition contains all subscribers active in Home networks in this condition.

roaming

Specifies the subscriber network access type as Roaming for condition validation in an IP-CAN session. This condition contains all subscribers active in Roaming networks in this condition.

visiting

Specifies the subscriber network access type as Visiting for condition validation in an IP-CAN session. This condition contains all subscribers active in Visiting networks in this condition.

Usage

Use this command to define a condition based on the location of the user in access type (Home/Roaming/Visiting) in an IP-CAN session as received on **Gx** interface.

Example

The following command creates a condition definition to analyze the condition based on location of the subscribes as **roaming** in an IP-CAN session:

```
user-access-network = roaming
```

user-equipment-info esn

This command defines a condition based on the Electronic Serial Number (ESN) used for the identification of mobile device (UE) in a Non-3GPP IP-CAN session received over **Gx** interface between PDSN and IPCF.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] user-equipment-info esn operator esn
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

esn

Specifies the Electronic Serial Number used for the identification of UE in 64 bit format as condition value for UE information received over **Gx** interface in a Non-3GPP IP-CAN session.
esn must be a 15 character long string of Hexadecimal numbers only.

Usage

Use this command to define a condition based on the ESN of the UE received over **Gx** interface in a Non-3GPP IP-CAN session between PDSN and IPCF.

Example

The following command creates a condition definition to analyze the condition based on the ESN of the UE as *1234567890120AF* in a Non-3GPP IP-CAN session:

```
user-equipment-info esn = 1234567890120AF
```

user-equipment-info eui64

This command defines a condition based on the Extended Unique Identifier in 64 bit (EUI-64) used for the identification of mobile device (UE) in an IP-CAN session received over **Gx** interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] user-equipment-info eui64 operator eui64
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

eui64

Specifies the Extended Unique Identifier in 64 bit format as a condition value for UE information received over **Gx** interface in an IP-CAN session.
eui64 is a 16 character long string of Hexadecimal numbers only.

Usage

Use this command to define a condition based on the EUI-64 value of the UE received over **Gx** interface in an IP-CAN session between PCEF and IPCF.

Example

The following command creates a condition definition to analyze the condition based on the EUI-64 of the UE as *0012989099832345* in an IP-CAN session:

```
user-equipment-info eui64 = 0012989099832345
```

user-equipment-info imeisv

This command defines a condition based on the International Mobile Equipment Identity Software Version (IMEI-SV) used for the identification of mobile device (UE) in an IP-CAN session received over **Gx** interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] user-equipment-info imeisv *operator imei_sv*

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

imei_sv

Specifies the International Mobile Equipment Identity Software Version (IMEI-SV) as a condition value for UE information received over **Gx** interface in an IP-CAN session.
eui64 is a 16 digit long string of decimal numbers only.

Usage

Use this command to define a condition based on the IMEI-SV value of the UE received over **Gx** interface in an IP-CAN session between PCEF and IPCF.

Example

The following command creates a condition definition to analyze the condition based on the IMEI-SV of the UE as *0012989099832345* in an IP-CAN session:

user-equipment-info eui64 = *0012989099832345*

user-equipment-info mac

This command defines a condition based on the Media Access Control (MAC) address used for the UE information in an IP-CAN session as received over **Gx** interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] user-equipment-info mac *operator mac_value*

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

mac_value

Specifies the Media Access Control (MAC) address as condition value for UE information received over **Gx** interface in an IP-CAN session.
mac_value is a 17 character long string of Hexadecimal numbers in *xx:xx:xx:xx:xx:xx* format only.

Usage

Use this command to define a condition based on the MAC address value as UE information received over **Gx** interface in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on the MAC value of the UE as *00:12:98:90:99:83* in an IP-CAN session:

```
user-equipment-info mac = 00:12:98:90:99:83
```

user-equipment-info meid

This command defines a condition based on the Mobile Equipment Id (MEID) used for the identification of CDMA mobile device (UE) in a Non-3GPP IP-CAN session received over **Gx** interface between PDSN and IPCF.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] user-equipment-info meid operator me_id
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

me_id

Specifies the Mobile Equipment identifier used for the identification of UE in 64 bit format as condition value for UE information received over **Gx** interface in a Non-3GPP IP-CAN session.
me_id must be a 14 character long string of Hexadecimal numbers only.

Usage

Use this command to define a condition based on the MEID of the CDMAUE received over **Gx** interface in a Non-3GPP IP-CAN session between PDSN and IPCF.

Example

The following command creates a condition definition to analyze the condition based on the MEID of the CDMA UE as *123456780120AF* in a Non-3GPP IP-CAN session:

```
user-equipment-info meid = 123456780120AF
```

user-equipment-info modified-eui64

This command defines a condition based on the modified-Extended Unique Identifier in 64 bit (EUI-64) used for the identification of mobile device (UE) in an IP-CAN session received over **Gx** interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] user-equipment-info modified-eui64 operator meui64
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

meui64

Specifies the modified Extended Unique Identifier (EUI) in 64 bit format as condition value for UE information received over **Gx** interface in an IP-CAN session.
meui64 is a 16 character long string of Hexadecimal numbers only.

Usage

Use this command to define a condition based on the modified EUI-64 value of the UE received over **Gx** interface in an IP-CAN session between PCEF and IPCF.

Example

The following command creates a condition definition to analyze the condition based on the EUI-64 of the UE as *0012989099832345* in an IP-CAN session:

```
user-equipment-info modified-eui64 = 0012989099832345
```

user-location-info

This command defines a condition based on the UE location used in an IP-CAN session as received on **Gx** interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] user-location-info {cgi operator mcc mcc_value mnc mnc_value lac lac_value ci
ci_value | ecgi operator mcc mcc_value mnc mnc_value ecgi ecgi_value | rai operator mcc
mcc_value mnc mnc_value lac lac_value rai rai_value| sai operator mcc mcc_value mnc
mnc_value lac lac_value sac sac_value| tai operator mcc mcc_value mnc mnc_value tai
tai_value}
```

no

Removes the specified condition definition.

cgi

Specifies the Cell Global Identifier in UE location received over **Gx** interface in an IP-CAN session.

ecgi

Specifies the E-UTRAN Cell Global Identifier in UE location received over **Gx** interface in an IP-CAN session.

rai

Specifies the Routing Area Identifier in UE location received over **Gx** interface in an IP-CAN session.

sai

Specifies the Service Area Identifier in UE location received over **Gx** interface in an IP-CAN session.

tai

Specifies the Tracking Area Identifier in UE location received over **Gx** interface in an IP-CAN session.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

mcc *mcc_value*

Specifies the Mobile Country Code used in UE location information received over **Gx** interface in IP-CAN session.
mcc_value must be an integer between 101 through 998.

mnc *mnc_value*

Specifies the Mobile Network Code used in UE location information received over **Gx** interface in IP-CAN session.
mnc_value must be an integer between 1 through 998.

lac *lac_value*

Specifies the Location Area Code used in UE location information received over **Gx** interface in IP-CAN session.
lac_value must be an integer between 1 through 65535.

ci *ci_value*

Specifies the Cell Identifier used in UE location information received over **Gx** interface in IP-CAN session.
ci_value must be an integer between 1 through 65535.

ecgi *ecgi_value*

Specifies the E-UTRAN Cell Global Identifier used in UE location information received over **Gx** interface in IP-CAN session.
ecgi_value must be an integer between 1 through 1048575.

rai *rai_value*

Specifies the Routing Area Identifier used in UE location information received over **Gx** interface in IP-CAN session.
rai_value must be an integer between 1 through 65535.

sac *sac_value*

Specifies the Service Area Code used in UE location information received over **Gx** interface in IP-CAN session.
sac_value must be an integer between 1 through 65535.

tai *tai_value*

Specifies the Tracking Area Code used in UE location information received over **Gx** interface in IP-CAN session.
tai_value must be an integer between 1 through 65535.

Usage

Use this command to define a condition based on the UE location information received over **Gx** interface in an IP-CAN session.

Example

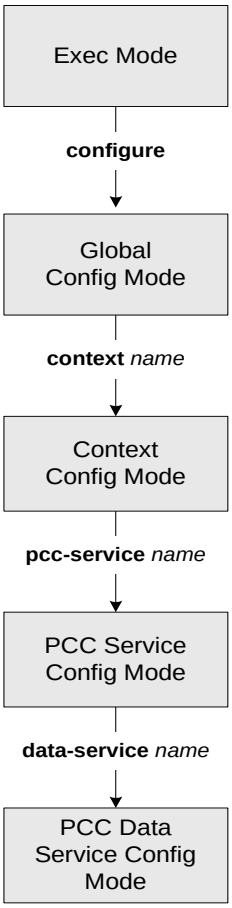
The following command creates a condition definition to analyze the condition based on the RAI received for UE location in an IP-CAN session:

```
user-location-info rai  = mcc 102 mnc 99 lac 1003 rai 3521
```

Chapter 218
PCC-Data-Service Configuration Mode Commands

The PCC-Data-Service Configuration Mode is used to configure the data flow parameters for the media data, as well as corresponding attributes that are necessary for charging and policy enforcement decisions for the media parameters represented by its service flows in the PCC-service. A maximum of ten service data flows can be configured in a PCC-Data-Service instance.

Important: This configuration mode is supported from StarOS Release 12.1 onward.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

flow direction in

This command configures the flow service parameters for incoming data flow in PCC-Data-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] flow direction in protocol {ip | tcp | udp} from {src_ip_addr | any} port
{src_port_num | any} to {dest_ip_addr | any} port {dest_port_num | any}
```

no

Removes the configured data service flow parameters from PCC-Data-Service instance for IPCF configuration.

protocol {ip | tcp | udp}

This keyword configures the data flow parameters for specific protocol.
Following protocols are supported through this keyword:

- **ip**: Sets the parameters for IP traffic.
- **tcp**: Sets the parameters for TCP traffic.
- **UDP**: Sets the parameters for UDP traffic.

from {*src_ip_addr* | any} port {*src_port_num* | any}

This keyword configures the data flow condition parameters for specific protocol through IP address and port as source of flow.
Following parameters are defined with this keyword:

- *src_ip_addr*: specifies the specific IP address in IPv4/IPv6 notation as source of flow.
- **any**: specifies that flow from any source IP address/port can be analyzed or considered.
- **port** *src_port_num*: specifies the specific source port parameter for flow.

  src_port_num is the source port number of flow and must be an integer from 1 through 65535.

to {*dest_ip_addr* | any} port {*dest_port_num* | any}

This keyword configures the data flow condition parameters for specific protocol through IP address and port as source of flow.
Following parameters are defined with this keyword:

- *dest_ip_addr*: specifies the specific IP address in IPv4/IPv6 notation as destination of flow.
- **any**: specifies that flow to any destination IP address/port can be analyzed or considered.
- **port** *dest_port_num*: specifies the specific destination port parameter for flow.

dest_port_num is the destination port number of flow and must be an integer from 1 through 65535.

Usage

Use this command to configure the flow service parameters for incoming data flow in PCC-Data-Service instance for IPCF Configuration.

Example

Following command sets the data service parameters for **tcp** type protocol from **any** IP/port source to **any** IP/port in incoming direction with in a PCC-Data-Service.

```
flow direction in protocol tcp from any port any to any port any
```

flow direction out

This command configures the flow service parameters for outgoing data flow in PCC-Data-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] flow direction in protocol {ip | tcp | udp} from {src_ip_addr | any} port
{src_port_num | any} to {dest_ip_addr | any} port {dest_port_num | any}
```

no

Removes the configured data service flow parameters from PCC-Data-Service instance on IPCF node.

protocol {ip | tcp | udp}

This keyword configures the data flow parameters for specific protocol.
Following protocols are supported through this keyword:

- **ip**: Sets the parameters for IP traffic.
- **tcp**: Sets the parameters for TCP traffic.
- **UDP**: Sets the parameters for UDP traffic.

from {*src_ip_addr* | any} port {*src_port_num* | any}

This keyword configures the data flow condition parameters for specific protocol through IP address and port as source of flow.
Following parameters are defined with this keyword:

- *src_ip_addr*: specifies the specific IP address in IPv4/IPv6 notation as source of flow.
- **any**: specifies that flow from any source IP address/port can be analyzed or considered.
- **port** *src_port_num*: specifies the specific source port parameter for flow.

  src_port_num is the source port number of flow and must be an integer from 1 through 65535.

to {*dest_ip_addr* | any} port {*dest_port_num* | any}

This keyword configures the data flow condition parameters for specific protocol through IP address and port as source of flow.
Following parameters are defined with this keyword:

- *dest_ip_addr*: specifies the specific IP address in IPv4/IPv6 notation as destination of flow.
- **any**: specifies that flow to any destination IP address/port can be analyzed or considered.
- **port** *dest_port_num*: specifies the specific destination port parameter for flow.

  dest_port_num is the destination port number of flow and must be an integer from 1 through 65535.

Usage

Use this command to configure the flow service parameters for outgoing data flow in PCC-Data-Service instance on IPCF node.

Example

Following command sets the data service parameters for **tcp** type protocol from **any** IP/port source to **any** IP/port in outgoing direction with in a PCC-Data-Service.

```
flow direction out protocol tcp from any port any to any port any
```

metering-method

This command specifies the metering method to be used by PCEF for offline charging in a PCC-Data-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] metering-method {both-duration-volume | duration | volume}
```

no

Removes the configured metering method from PCC-Data-Service instance on IPCF node.
In such scenario, the metering method pre-configured at PCEF is considered.

both-duration-volume

Specifies the metering method as based on volume of data usage and duration of session, both for offline charging in a PCC-Data-Service instance on IPCF node.

duration

Specifies the metering method as based on the duration of session usage for offline charging in a PCC-Data-Service instance on IPCF node.

volume

Specifies the metering method as based on the volume of data usage for offline charging in a PCC-Data-Service instance on IPCF node.

Usage

Use this command to define the metering method to be used for offline charging in a PCC-Data-Service instance on IPCF node.
If no metering method is defined, the metering method preconfigured at PCEF is considered.

Example

Following command sets the metering method as based on volume of data usage and duration of session, both for offline charging in a PCC-Data-Service instance on IPCF node.

```
metering-method both-duration-volume
```

monitoring-key

This command defines the monitoring key under which data is monitored for the PCC-Data-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

monitoring-key *mon_key_value*

[**no**] **monitoring-key**

no

Removes the configured monitoring-key from PCC-Data-Service instance on IPCF node.

mon_key_value

Specifies the monitoring key value under which data usage is monitored for the PCC-Data-Service instance and must be an integer from 1 through 65535.

Usage

Use this command to define the monitoring key under which data is monitored for the PCC-Data-Service instance on IPCF node.

Example

Following command sets the monitoring key *123* for data monitoring in PCC-Data-Service instance on IPCF node.

```
monitoring-key 123
```

precedence

This command defines the precedence that is assigned to the Dynamic PCC rule created for a PCC-Data-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

precedence *preced_value*

[**no**] **precedence**

no

Removes the configured precedence value from PCC-Data-Service instance on IPCF node.

preced_value

Specifies the precedence that is assigned to the dynamic PCC rule created for a PCC-Data-Service instance and must be an integer from 1 through 65535.

Usage

Use this command to define the precedence value that is assigned to the Dynamic PCC rule created for a PCC-Data-Service instance on IPCF node.

Example

Following command sets the precedence value*2* to assign to the dynamic PCC rule created for a PCC-Data-Service instance on IPCF node.

```
precedence 2
```

qos-profile

This command defines the PCC-QoS-Profile which is to use for the PCC-Data-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

qos-profile *qos_prof_name*

[**no**] **qos-profile**

no

Removes the configured PCC-QoS-Profile from PCC-Data-Service instance on IPCF node.

qos_prof_name

Specifies the pre-configured PCC-QoS-Profile name which is to use for the PCC-Data-Service instance.

Usage

Use this command to define the PCC-QoS-Profile for a PCC-Data-Service instance on IPCF node.

Example

Following command sets the PCC-QoS-Profile *ipcf_qos_prof1* for PCC-Data-Service instance on IPCF node.

```
qos-profile ipcf_qos_prof1
```

rating-group

This command defines the PCC-Rating-Group that is assigned for a PCC-Data-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

rating-group *rating_grp_id*

[**no**] **rating-group**

no

Removes the configured PCC-Rating-Group Id from PCC-Data-Service instance on IPCF node.

rating_grp_id

Specifies the PCC-Rating-Group Id that is assigned to the PCC-Data-Service instance and must be an integer from 1 through 99.

Usage

Use this command to define the PCC-Rating Id value for a PCC-Data-Service instance on IPCF node.

Example

Following command sets the Rating Group id *11* for a PCC-Data-Service instance on IPCF node.

```
rating-group 11
```

reporting-level

This command specifies the reporting level to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] reporting-level {service-identifier-level | rating-group-level}
```

no

Removes the configured usage reporting level from PCC-Data-Service instance on IPCF node.
In such scenario, the reporting level configured at PCEF is considered.

service-identifier-level

Sets the data usage reporting level to be used by PCEF to report the data usage for the related PCC rule at the service identifier level in a PCC-Data-Service instance on IPCF node.

rating-group-level

Sets the data usage reporting level to be used by PCEF to report the data usage for the related PCC rule at the Rating-group level in a PCC-Data-Service instance on IPCF node.

Usage

Use this command to define the reporting level to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-Service instance on IPCF node.
If no reporting level is defined, the reporting level preconfigured at PCEF is considered.

Example

Following command sets the reporting level at 'Rating-group' level which is to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-Service instance on IPCF node.

```
reporting-level rating-group-level
```

service-identifier

This command defines the service identifier for a PCC-Data-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

service-identifier *svc_id*

[**no**] **service-identifier**

no

Removes the configured Service Identifier from PCC-Data-Service instance on IPCF node.

svc_id

Specifies the Service Identifier that is assigned to the PCC-Data-Service instance and must be an integer from 1 through 65535.

Usage

Use this command to define the Service Identifier for a PCC-Data-Service instance on IPCF node.

Example

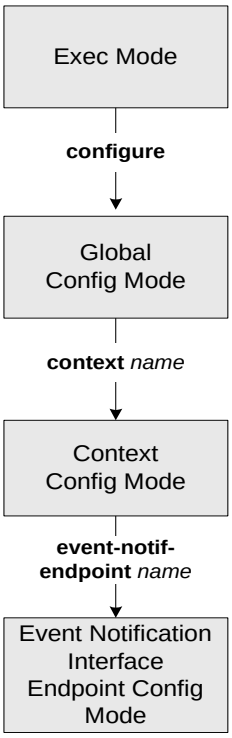
Following command sets the Service Identifier *1011* for a PCC-Data-Service instance on IPCF node.

service-identifier *1011*

Chapter 219
PCC-Event-Notification-Interface-Endpoint Configuration Mode Commands

The PCC-Event-Notification-Interface-Endpoint configuration mode is used to enable the event notification interface mechanism for the Intelligent Policy Control Function (IPCF) and to configure the Event Notification collection server endpoint related parameters.

Important: This configuration mode is supported from StarOS Release 12.1 onward.



address

This command binds an IP address to the local IPCF node which is to be used for event notification processing with remote event collection server endpoint during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

address *ip_address*

ip_address

Specifies the IP address bind with local IPCF node to be used by the event collection server endpoint for event message processing during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Usage

Use this command to bind an IP address to interact with the remote event notification collection server endpoint to which the event messages are sent for IP-CAN session events.

Example

Following command binds the *1.2.3.4* for event notification message with remote event notification endpoint.

address*1.2.3.4*

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

peer name

This command binds/associates a remote Event Notification collection server as peer having specified IP address and optionally port for event notification during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

peer name *peer_name* **address** *ip_address* [**port** *port_num*]

name *peer_name*

Sets the in PCC-Event-Notification-Interface-Endpoint instance to use a particular peer node configured by a peer name *peer_name* for event notification interface.
The *peer_name* is name of the peer node to be sued for event collection and must be an alphanumerical string from 1 through 31 characters. *peer_name* allows punctuation marks.

ip-address *ip_address*

Sets the PCC-Event-Notification-Interface-Endpoint instance to bind the particular peer node name with IP address *ip_address* in IPv4 or IPv6 notation for event notification message processing.
The *ip_address* is an IP address in IPv4/IPv6 notation.

port *port_num*

This optional keyword sets a particular port number to be used with in the PCC-Event-Notification-Interface-Endpoint instance to configure a particular peer node having a pre assigned IP address *ip_address* in IPv4 or IPv6 notation for event notification message processing.
The *port_num* must be an integer between 1 and 65535.

Usage

Use this command to bind/associate a remote Event Notification collection server as peer having specified IP address and optionally port for event notification during IP-CAN session in the PCC-Event-Notification-Interface-Endpoint instance.
Multiple peers can be configured using this command and peer selection methods, **primary-secondary** or **round-robin** can be applied using **peer select-algorithm** command for event notification during IP-CAN session in this configuration mode.

Example

Following command configures and associates an Event Notification peer node named *event_peer_1* having an IP address *1.2.3.4* with port number as *2345* in an PCC-Event-Notification-Interface-Endpoint instance.

```
peer name event_peer_1 ip-address 1.2.3.4 port 2345
```

peer select-algorithm

This command applies the peer selection algorithm to select the configured remote Event Notification collection server during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
peer select-algorithm {primary-secondary | round-robin}
```

primary-secondary

Sets the PCC-Event-Notification-Interface-Endpoint peer selection algorithm to select the configured remote peer servers in primary and secondary method during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.
This mode is applicable only when multiple peers are configured and primary and secondary peer is defined using **peer select-peer** command in this configuration mode.

round-robin

Sets the PCC-Event-Notification-Interface-Endpoint peer selection algorithm to select the configured remote peer servers in round-robin method mode during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.
This mode is applicable only when multiple peers are configured in this configuration mode.

Usage

Use this command apply the peer selection algorithm to select the configured remote Event Notification collection server during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Example

Following command configures the peer selection algorithm to select the configured remote peer in **round-robin** method in PCC-Event-Notification-Interface-Endpoint instance.

```
peer select-algorithm round-robin
```

Following command configures the peer selection algorithm to select the configured primary and secondary remote peers in **primary-secondary** method in PCC-Event-Notification-Interface-Endpoint instance.

```
peer select-algorithm primary-secondary
```

peer select-peer

This command sets the configured remote Event Notification collection server as primary and secondary servers for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

peer select-peer *pri_peer_name* **secondary** *sec_peer_name*

pri_peer_name

Sets the configured remote PCC-Event-Notification-Interface-Endpoint peer as primary peer for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance. *pri_peer_name* must be a pre-configured peer name configured with **peer name** command in this configuration mode.

secondary *sec_peer_name*

Sets the configured remote PCC-Event-Notification-Interface-Endpoint peer as secondary peer for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance. *sec_peer_name* must be a pre-configured peer name configured with **peer name** command in this configuration mode.

Usage

Use this command to set the configured remote Event Notification collection server as primary and secondary node for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.
This configuration is used when peer selection algorithm is set to **primary-secondary** using **peer select-algorithm** command in this configuration mode.

Example

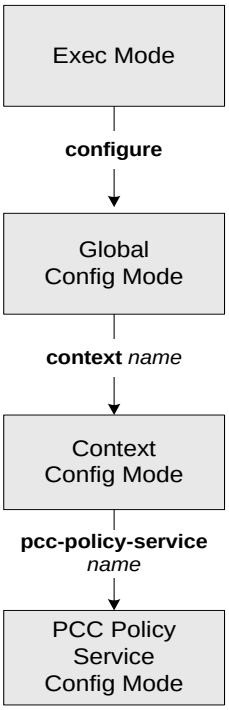
Following command configures the specified peer *event1* as primary and *event2* as secondary node for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

```
peer select-peer event1 secondary event2
```

Chapter 220
PCC-Policy-Service Configuration Mode Commands

The PCC-Policy-Service Configuration mode provides a mechanism for the Intelligent Policy Control Function (IPCF) to manage the external interfaces required for policy authorization purpose between IPCF and PCEF Bearer Binding and Event Reporting Function (BBERF). The PCC-Policy-Service manages **Gx**/**Gx** based on the Diameter dictionary used.

Important: This configuration mode is supported from StarOS Release 12.1 onward.



associate pcc-service

This command associates a pre-configured PCC-Service with a PCC-Policy-Service for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

associate pcc-service *pcc_service_name*

[**no**] **associate pcc-service**

no

Removes/disassociate the configured PCC-Service from this PCC-Policy-Service instance configured for IPCF configuration.

pcc_service_name

Specifies the name of a pre-configured PCC-Service configured in Context Configuration mode for IPCF configuration.
The *pcc_service_name* is name of a predefined PCC-Service instance and must be an alphanumerical string from 1 through 63 characters.

Usage

Use this command to associate a pre-configured PCC-Service instance for IPCF configuration.

Important: For more information on PCC-Service configuration, refer *PCC-Service Configuration Mode Commands*.

Example

Following command binds a PCC-Service named *pcc_svc1* with in a PCC-Policy-Service.

associate pcc-service *pcc_svc1*

Following command removes an associated PCC-Service named *pcc_svc1* from a PCC-Policy-Service.

no associate pcc-service *pcc_svc1*

diameter dictionary

This command assigns a Diameter dictionary for **Gx**/**Gxa** messaging with a PCC-Policy-Service for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

diameter dictionary {**gxa-standard** | **r7-standard** | **standard**}

default diameter dictionary

default

Sets the Diameter **Gx** dictionary to default dictionary **standard** (3GPP Rel. 8 standard) for a PCC-Policy-Service instance configured for IPCF configuration.

gxa-standard

Default: Disabled
Sets the Diameter **Gxa** dictionary to be used by a PCC-Policy-Service instance configured for IPCF configuration over **Gxa** interface to 3GPP Rel. 8 standard.

r7-standard

Default: Disabled
Sets the Diameter **Gx** dictionary to be used by a PCC-Policy-Service instance configured for IPCF configuration over **Gx** interface to 3GPP Rel. 7 standard.

standard

Default: Enabled
Sets the Diameter **Gx** dictionary to be used by a PCC-Policy-Service instance configured for IPCF configuration over **Gx** interface to 3GPP Rel. 8 standard.

Usage

Use this command to configure the PCC-Policy-Service to determine which of the 3GPP dictionary to be used for **Gx** or **Gxa** interface messaging for policy and/or quota management.

Example

Following command sets the PCC-Policy-Service to use 3GPP Rel. 8 standard dictionary for **Gx** interface and policy management related messaging in a PCC-Policy-Service.

```
default diameter dictionary
```

diameter origin end-point

This command binds/associates a pre-configured Diameter host/realm (PCEF/BBERF) over **Gx/Gxa** interface with a PCC-Policy-Service to be used for subscriber service control and policy profile management.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

diameter origin endpoint *dia_endpoint_name*

no diameter origin endpoint

no

Removes the associated Diameter Origin Endpoint configuration from PCC-Policy-Service instance configured for IPCF configuration.

any

Sets the PCC-Policy-Service instance to use any available PCEF/BBERF node for policy interfaces (**Gx**/**Gx**-like) support.

dia_endpoint_name

The *dia_endpoint_name* is a predefined Diameter origin endpoint node and must be an alphanumerical string from 1 through 63 characters.

Usage

Use this command to bind the PCEF/BBERF node over **Gx**/**Gx**-like interface by associating a pre-configured Diameter Origin Endpoint with a PCC-Policy-Service.
The Diameter origin endpoint must be a pre-configured instance in the Context Configuration Mode. For more information on Diameter origin endpoint configuration, refer *Diameter Endpoint Configuration Mode Commands* chapter.

Example

Following command associates a pre-configured Diameter endpoint node configuration named *pcef_1* with a PCC-Policy-Service for policy profile management.

```
diameter origin endpointpcef_1
```

Following command removes the pre-associated Diameter endpoint node configuration named *pcef_1* with a PCC-Policy-Service.

```
no diameter origin endpoint
```

ehrpd-access-bcm

This command configures the PCC-Policy-Service to accept the applicable Bearer-Control-Mode for eHRPD access over **Gxa** interface on IPCF.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

ehrpd-access-bcm {**as-requested** | **ue-nw** | **ue-only**}

default ehrpd-access-bcm

default

Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from Application Server (AS) for eHRPD access over **Gxa** interface on IPCF node.

as-requested

Default: Enabled.
Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from Application Server (AS) for eHRPD access over **Gxa** interface on IPCF node.

ue-nw

Default: Disabled.
Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from UE and/or network element for eHRPD access over **Gxa** interface on IPCF node.

ue-only

Default: Disabled.
Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from UE only for eHRPD access over **Gxa** interface on IPCF node.

Usage

Use this command to set the PCC-Policy-Service to accept the Bearer-Control-Mode request from AS or UE or Network for eHRPD access over **Gxa** interface on IPCF node.

Example

Following command sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from AS for eHRPD access over **Gxa** interface on IPCF node.

```
default ehrpd-access-bcm
```

Following command sets the PCC-Policy-Service to accept the Bearer-Control-Mode request only from UE for eHRPD access over **Gxa** interface on IPCF node.

```
ehrpd-access-bcm ue-only
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

gprs-access-bcm

This command configures the PCC-Policy-Service to accept the applicable Bearer-Control-Mode for GPRS access over **Gx** interface on IPCF.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
gprs-access-bcm {as-requested | ue-nw | ue-only}

default gprs-access-bcm
```

default

Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from Application Server (AS) for GGSN access over **Gx** interface on IPCF node.

as-requested

Default: Enabled.
Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from Application Server (AS) for GGSN access over **Gx** interface on IPCF node.

ue-nw

Default: Disabled.
Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from UE and/or network element for GGSN access over **Gx** interface on IPCF node.

ue-only

Default: Disabled.
Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from UE only for GGSN access over **Gx** interface on IPCF node.

Usage

Use this command to set the PCC-Policy-Service to accept the Bearer-Control-Mode request from AS or UE or Network for GGSN access over **Gx** interface on IPCF node.

Example

Following command sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from AS for GGSN access over **Gx** interface on IPCF node.

```
default gprs-access-bcm
```

Following command sets the PCC-Policy-Service to accept the Bearer-Control-Mode request only from UE for GGSN access over **Gx** interface on IPCF node.

```
gprs-access-bcm ue-only
```

max policy-sessions

This command configures the maximum limit of the policy sessions allowed in a PCC-Policy-Service instance on IPCF.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

max policy-sessions *max_session*

default max policy-sessions

default

Sets the maximum policy sessions allowed in PCC-Policy-Service instance to default value of 10000 sessions.

max_session

Default: 10000
Specifies the maximum number of policy sessions configured in PCC-Policy-Service to allow to be connected in PCC-Quota service instance.
max_session must be an integer between 0 and 4000000.

Usage

Use this command to set the maximum number of policy sessions allowed by a PCC-Policy-Service instance on IPCF.

Example

Following command sets the maximum number of policy sessions allowed in PCC-Policy-Service instance to 10000.

```
default max policy-sessions
```

subscriber-binding-identifier

This command specifies the subscriber binding identifier to be used by **bindmux** for binding different subscriber session to PCC-Policy-Service on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

subscriber-binding-identifier {**imsi** | **msisdn** | **nai** | **sip-uri**}

default subscriber-binding-identifier

default

Sets the subscriber binding identifier to default value; i.e. IMSI, to be used by **bindmux** for binding different subscriber session to PCC-Policy-Service on IPCF node.

imsi

Default: Enabled.
Sets the subscriber binding identifier as IMSI to be used by **bindmux** for binding different subscriber session to PCC-Policy-Service on IPCF node.

msisdn

Default: Disabled.
Sets the subscriber binding identifier as MSISDN to be used by **bindmux** for binding different subscriber session to PCC-Policy-Service on IPCF node.

nai

Default: Disabled.
Sets the subscriber binding identifier as Network Access Identifier (NAI) to be used by **bindmux** for binding different subscriber session to PCC-Policy-Service on IPCF node.

sip-uri

Default: Disabled.
Sets the subscriber binding identifier as SIP URI (Uniform Resource Identifier) to be used by **bindmux** for binding different subscriber session to PCC-Policy-Service on IPCF node.

Usage

Use this command to configure the **bindmux** in PCC-Policy-Service instance on IPCF node to use specific subscriber identifier for binding different subscriber session to IP-CAN session.

Example

The following command sets the PCC-Policy-Service to use IMSI as subscriber binding identifier for IP-CAN session on an IPCF node.

```
default subscriber-binding-identifier
```

subscription-id-absence-action

This command configures the PCC-Policy-Service instance to handle the Initial Credit Control Request (CCR-I) messages during initial authentication over **Gx** interface when CCR-I message received by IPCF node is without a valid Subscription-Id AVP (IMSI, NAI, E164 etc.).

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
{default} subscription-id-absence-action initial-auth {continue | reject}
```

default

Sets the PCC-Policy-Service instance to reject the CCR-I message during initial authentication over **Gx** interface if received without a valid Subscription-Id AVP (IMSI, NAI, E164 etc.) on IPCF node.

continue

Default: Disabled.
Sets the PCC-Policy-Service instance to accept the CCR-I message and continue with the session if CCR-I is received without a valid Subscription-Id AVP (IMSI, NAI, E164 etc.) on IPCF node.
In this case, IPCF accepts the CCR-I message and will do the PCC provisioning as per the operator configuration in associated PCC-Service.

reject

Default: Enabled.
Sets the PCC-Policy-Service instance to reject the CCR-I message and continue with the session if CCR-I is received without a valid Subscription-Id AVP (IMSI, NAI, E164 etc.) on IPCF node.
In this case, IPCF will send CCA-I message with Result-code as **Permanent Error** and rejects the session establishment with PCEF.

Usage

Use this command to configure the PCC-Policy-Service instance to handle the Initial Credit Control Request (CCR-I) message processing during the initial authentication over **Gx** interface if CCR-I message received by IPCF node has no valid Subscription-Id AVP.

Example

The following command sets the PCC-Policy-Service to reject the CCR-I request and terminations the session establishment with PCEF.

```
default subscription-id-absence-action initial-auth
```

unsolicited-provisioning

This command is used to enable/disable the support for unsolicited time-of-day-based procedures to PCC-Policy-Service on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no | default] unsolicited-provisioning time-of-day
```

default

Sets the support for unsolicited time-of-day-based procedures to default mode; i.e. disabled, in PCC-Policy-Service instance on IPCF node.

no

Removes the configured support for unsolicited time-of-day-based procedures in PCC-Policy-Service instance on IPCF node.

Usage

Use this command to enable/disable the support for unsolicited time-of-day-based procedures to PCC-Policy-Service on IPCF node.
By default this command is disabled.

Example

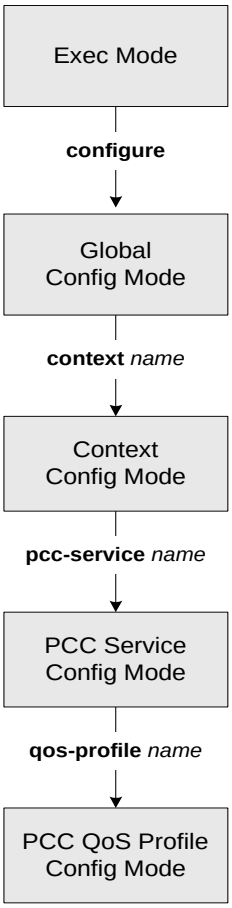
The following command enables the unsolicited time-of-day-based procedures to PCC-Policy-Service on an IPCF node.

```
unsolicited-provisioning time-of-day
```

Chapter 221
PCC-QoS-Profile Configuration Mode Commands

The PCC-QoS-Profile Configuration Mode is used to define the QoS logic used by the operator for managing the QoS policy requirements and objectives for the network specific to a group of subscribers in the network. A QoS Profile represents a resource requirement identified by means of the corresponding QoS attributes like QCI, MBR, GBR, ARP etc.

Important: This configuration mode is supported from StarOS Release 12.1 onward.



arp-priority

This command is used to define the Allocation and Retention Priority (ARP) values of the QoS profile in PCC-QoS-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] arp-priority arp_priority pre-emption {capable | not-capable} {not-vulnerable | vulnerable}
```

no

Removes the configured ARP priority set for PCC-QoS-Profile for PCC-Service instance on IPCF node.

arp_priority

Specifies the priority value for ARP in a PCC-QoS-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.
arp_priority must be an integer from 1 through 15.

pre-emption {capable | not-capable}

Sets the Pre-emption capability related parameters with ARP priority in PCC-QoS-Profile name which is to use in Subscriber profile in PCC-Service instance on IPCF node.
Pre-emption capability determines whether a bearer with a lower ARP priority level should be dropped to free up the required resources.
capable: This keyword indicates that the service data flow is allowed to get resources that were already assigned to another service data flow with a lower priority level.
non-capable: This keyword indicates that the service data flow is not allowed to get resources that were already assigned to another service data flow with a lower priority level.

{not-vulnerable | vulnerable}

Sets the Pre-emption vulnerability related parameters with ARP priority in PCC-QoS-Profile name which is to use in Subscriber profile in PCC-Service instance on IPCF node.
Pre-emption vulnerability determines whether a bearer is applicable for dropping by a pre-emption capable bearer with a higher ARP priority value.
not-vulnerable: This keyword indicates that the resources assigned to the service data flow shall not be pre-empted and allocated to a service data flow with a higher priority level.
vulnerable: This keyword indicates that the resources assigned to the service data flow can be pre-empted and allocated to a service data flow with a higher priority level.

Usage

Use this command to define the ARP priority and pre-empt parameters in PCC-QoS-Profile which is to be used in Subscriber profile in PCC-Service instance on IPCF node.
ARP controls how the IPCF reacts when there are insufficient resources to establish the new RAB. Typically it manages it by; 1) Deny the RAB request and 2) Preempt an existing RAB and accept the new RAB request.

Example

Following command sets the ARP Priority *2* with preemption capability and vulnerability in PCC-QoS-Profile instance on IPCF node.

```
arp-priority 2 pre-emption capable vulnerable
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

guaranteed-bitrate

This command defines the Guaranteed Bit Rate (GBR) value in bits per second for downlink and uplink traffic in PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] guaranteed-bitrate downlink downlink_gbr uplink uplink_gbr
```

no

Removes the configured GBR value set for PCC-QoS-Profile for PCC-Service instance on IPCF node.

downlink *downlink_gbr*

Sets the Guaranteed Bit Rate allowed in downlink direction (from PCEF to UE) in bits per second for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.
downlink_gbr must be an integer from 0 through 104857600. A 'zero' value disables the downlink in specified PCC-QoS-Profile.

uplink *uplink_gbr*

Sets the Guaranteed Bit Rate allowed in uplink direction (from PCEF to PDN) in bits per second for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.
uplink_gbr must be an integer from 0 through 104857600. A 'zero' value disables the uplink in specified PCC-QoS-Profile.

Usage

Use this command to define the Guaranteed Bit Rate value in bits per second for downlink and uplink traffic in PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

Example

Following command sets the *1024* bits per seconds as uplink GBR and *2048* bits per second as downlink GBR in PCC-QoS-Profile instance on IPCF node.

```
guaranteed-bitrate downlink 2048 uplink 1024
```

max-bitrate

This command defines the Maximum Bit Rate (MBR) value in bits per second for downlink and uplink traffic in PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

[no] max-bitrate downlink *downlink_mbr* **uplink** *uplink_mbr*

no

Removes the configured Maximum Bit Rate value set for PCC-QoS-Profile for PCC-Service instance on IPCF node.

downlink *downlink_mbr*

Sets the Maximum Bit Rate allowed in downlink direction (from PCEF to UE) in bits per second for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.
downlink_mbr must be an integer from 0 through 104857600. A 'zero' value disables the downlink in specified PCC-QoS-Profile.

uplink *uplink_mbr*

Sets the Maximum Bit Rate allowed in uplink direction (from PCEF to PDN) in bits per second for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.
uplink_mbr must be an integer from 0 through 104857600. A 'zero' value disables the uplink in specified PCC-QoS-Profile.

Usage

Use this command to define the Maximum Bit Rate value in bits per second for downlink and uplink traffic in PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

Example

Following command sets the *1024* bits per seconds as uplink MBR and *2048* bits per second as downlink MBR in PCC-QoS-Profile instance on IPCF node.

```
max-bitrate downlink 2048 uplink 1024
```

qci

This command sets the QoS Class Identifier (QCI) for PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] qci qci_id
```

no

Removes the configured QCI value set for PCC-QoS-Profile for PCC-Service instance on IPCF node.

qci *qci_id*

Sets the QoS Class Identifier for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.
qci_id must be an integer from 1 through 255.

Usage

Use this command to set the QoS Class Identifier for PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

Example

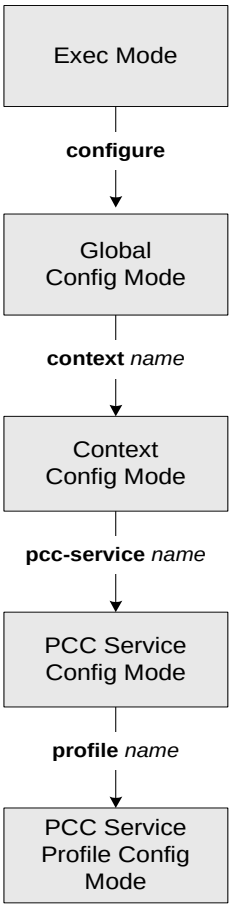
Following command sets the QCI *101* for PCC-QoS-Profile instance on IPCF node.

```
qci 101
```

Chapter 222
PCC-Service-Profile Configuration Mode Commands

The PCC-Service-Profile Configuration Mode is used to define the business logic used by the operator for managing the policy requirements and objectives for the network specific to a group of subscribers in the network. A PCC-Service-Profile manages multiple PCC-Conditions-Groups and associated PCC-Action-Sets pairs in an ordered manner. A maximum of 32 PCC-Service-Profile can be configured in a PCC-Service instance.

Important: This configuration mode is supported from StarOS Release 12.1 onward.



default-rulebase-name

This command is used to associate the default PCC-Rulebase with a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

[**no**] **default-rulebase-name** *rulebase_name*

no

Removes the configured default PCC-Rulebase from PCC-Service-Profile instance on IPCF node.

rulebase_name

This keyword specifies the default PCC-Rulebase name to be associated with PCC-Service-Profile instance. *rulebase_name* is the Rulebase name configured at PCEF and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to associate the default PCC-Rulebase configured on PCEF with a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Example

Following command associates the PCC-Rulebase named *pcc_rulebase1* for PCC-Profile instance on IPCF node.

```
default-rulebase-name pcc_rulebase1
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

eval-priority

This command sets the priority for evaluation of PCC-Condition-Group with corresponding PCC-Action-Set in a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] eval-priority last action-set actionset_name

[no] eval-priority priority_value timedef timedef_name [condition-group cond_grp_name]
action-set actionset_name

[no] eval-priority priority_value condition-group cond_grp_name action-set actionset_name
```

no

Removes the configured evaluation priority for PCC-Condition-Group with corresponding PCC-Action-Set from PCC-Service-Profile instance on IPCF node.

last

Sets last evaluation priority action-set configured for the PCC-Service-Profile instance.
no removes the last evaluation priority action-set.

priority_value

Specifies the priority to be set for PCC-Condition-Group with corresponding PCC-Action-Set in a PCC-Service-Profile instance.
priority_value must be an integer from 1 through 1023.

timedef *timedef_name*

Specifies a pre-configured time definition in *PCC-Timedef Configuration mode* and to be set for evaluation priority in a PCC-Service-Profile instance.
timedef_name is a pre-configured PCC-Timedef and must be an alphanumerical string of 1 through 63 characters.

condition-group *cond_grp_name*

Specifies a pre-configured PCC-Condition-Group to be set for evaluation priority in a PCC-Service-Profile instance.
cond_grp_name is a pre-configured PCC-Condition-Group and must be an alphanumerical string of 1 through 63 characters.

Important: An special PCC-Condition-Group “none” can be used to set the default PCC-Condition-Group for **any-match** typically used for a default condition for a session which does not match any of the conditions specified with higher evaluation priority.

action-set *actionset_name*

Specifies a pre-configured PCC-Action-Set for PCC-Condition-Group to be set for evaluation priority in a PCC-Service-Profile instance.
actionset_name is a pre-configured PCC-Action-Set and must be an alphanumerical string of 1 through 63 characters.

Usage

Use this command to set the priority for evaluation of PCC-Condition-Group with corresponding PCC-Action-Set in a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.
Additionally **timedef** is used to accept the Timedefs to support the time-of-day-based procedures to trigger an evaluation priority. The action is triggered only when the time of session lies in the time span defined in specific PCC-Timedef *timedef_name*.
Default **eval-priority** has the lowest priority in the PCC-Service-Profile and as default **eval-priority** does not have any PCC-Condition-Group associated with it, all the actions in the **action-set** always be applied.
A maximum of 64 PCC-Evaluation-Priorities can be configured in a PCC-Service-Profile.

Example

Following command sets the evaluation priority value as *1* for PCC-Condition-Group *cond_1* along with PCC-Action-Set *act_cond1* for PCC-Service-Profile instance on IPCF node:

```
eval-priority 1 condition-group cond_1 action-set act_cond1
```

Following command sets the evaluation priority value as *2* for PCC-Condition-Group *none* for **any-match** typically used for a default condition for a session which does not match any of the conditions specified with higher evaluation priority.along with PCC-Action-Set *act_cond1* for PCC-Service-Profile instance on IPCF node:

```
eval-priority 1 condition-group none action-set act_cond1
```

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

service-tag

This command configures the PCC-Service Tags to be used for PCC-Rulename or PCC-Rule-base in a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

[no] service-tag *svc_tag* {**rule-name** *rule_name* | **rulebase-name** *rulebase_name*}

no

Removes the configured PCC-Service Tags for PCC-Rulename and PCC-Rulebase from PCC-Service-Profile instance on IPCF node.

svc_tag

Specifies the name of the PCC-Service Tag to be used for PCC-Rulename and PCC-Rulebase in a PCC-Service-Profile instance.
svc_tag must be an alphanumerical string of 1 through 63 characters.

rule-name *rule_name*

Specifies a pre-defined PCC-Rulename on PCEF to be used with PCC-Service Tag *svc_tag* in a PCC-Service-Profile instance.
rule_name is a pre-defined PCC-Rulename on PCEF and must be an alphanumerical string of 1 through 63 characters.

rulebase-name *rulebase_name*

Specifies a pre-defined PCC-Rulebase name pre-defined on PCEF to be used with PCC-Service Tag *svc_tag* in a PCC-Service-Profile instance.
rulebase_name is a pre-defined PCC-Rulebase name on PCEF and must be an alphanumerical string of 1 through 63 characters.

Usage

Use this command to set the PCC-Service Tag for PCC-Rulename and PCC-Rulebase which are defined on PCEF with a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance.

Example

Following command sets the PCC-Service Tag named *Rule1* for PCC-Rulebase named *pcc_rulebase1* for PCC-Service-Profile instance on IPCF node:

```
service-tag Rule1 rulebase-name pcc_rulebase1
```

Following command sets the PCC-Service Tag named *Rule11* for PCC-Rulename *pcc_rule1* for PCC-Service-Profile instance on IPCF node:

service-tag *Rule11* **rule-name** *pcc_rule1*

usage-monitor

This command creates/modifies/deletes the PCC-Usage-Monitor Configuration instance to track the usage volume across the PCC-services based on the usage monitor settings in a PCC-service instance for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] usage-monitor usage_mon_name [-noconfirm]
```

no

Removes the configured PCC-Usage-Monitor from PCC-Service-Profile instance for IPCF configuration.

usage_mon_name

Identifies the name of the PCC-Usage-Monitor instance which is to be created or modified through this command.
The *usage_mon_name* must be an alphanumerical string from 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

WARNING: If this keyword option is used with **no usage-monitor** *usage_mon_name* command, the PCC-Usage-Monitor instance named *usage_mon_name* is deleted with all configured parameters without prompting any warning or confirmation.

Usage

Use this command to create and configure a PCC-Usage-Monitor for PCC-Service-Profile in a PCC-service instance of IPCF configuration.
A maximum number of 8 PCC-Usage-Monitors can be configured per PCC-Service-Profile.
Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-profile-usage-mon)#
```

The commands configured in this mode are defined in the *PCC-Usage-Monitor Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Caution: This is a critical configuration. The PCC-Usage-Monitor for volume usage can not be configured without this configuration. Any change to this configuration would lead to removing or disabling configuration parameters defined here.

Example

Following command configures the PCC-Usage-Monitor named *pcc_usage1* to track the usage of service with in a PCC-Service-Profile instance.

usage-monitor *pcc_usage1*

unknown-services-treatment

This command configures the PCC-Service for handling of unknown services at IPCF which is to be used in Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[default] unknown-services-treatment {not-allowed | qos-profile qos_prof_name precedence
from start_preced to end_preced order {ascending | descending}}
```

default

Sets the configured PCC-Service for handling of unknown services at IPCF to default value of "**Not allowed**" which is to be used in Subscriber profile in PCC-Service instance on IPCF node.

not-allowed

Sets the PCC-Service-Profile instance to reject the packet filters and does not installs any dynamic rule when IPCF receives any request to authorize Packet Filters from PCEF and no matching service flow is found in data service list.

qos-profile *qos_prof_name*

Specifies a pre-defined PCC-QoS profile name to be used to create dynamic rule when IPCF receives any request to authorize Packet Filters from PCEF and no matching service flow is found in data service list.
qos_prof_name is a pre-defined PCC-QoS Profile and must be an alphanumerical string of 1 through 63 characters.

precedence from *start_preced* **to** *end_preced*

Specifies the precedence parameters to install dynamic rules for selection of QoS profile when QoS profile is configured to create dynamic rule when IPCF receives any request to authorize Packet Filters from PCEF and no matching service flow is found in data service list.
start_preced is an integer between 1 through 65535 and must be less than *end_preced* value where *end_preced* is an integer between 1 through 65535 and must be more than *start_preced* value

order {ascending | descending}

Specifies the order of precedence for QoS profile to be used to install dynamic rule when IPCF receives any request to authorize Packet Filters from PCEF and no matching service flow is found in data service list.

- **ascending** sets the precedence setting in ascending order.
- **descending** sets the precedence setting in descending order.

Usage

Use this command to set the PCC-Service Tag for PCC-Rulename and PCC-Rulebase which are defined on PCEF with a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance.

Whenever IPCF receives any request to authorize Packet Filters from PCEF, it does a lookup in data service list to find a match. If **No** service flow is found matching then the requested filters are treated as **unknown service request** and handled as per the mentioned configuration.
When unknown-service-treatment is set to **not-allowed**, then Packet Filters are rejected and no dynamic rule is installed. Otherwise, dynamic rule is created using the requested packet filters, data rates mentioned in the QoS profile name *qos_prof_name* and precedence value derived from the configured values.
The precedence configuration works in following manner:

- If precedence limits are configured as 1000 to 2000 with order **ascending** then precedence of subsequent dynamic rules will go from 1000 to 2000.
- If precedence limits are configured as 1000 to 2000 with order **descending** then precedence of subsequent dynamic rules will go from 2000 to 1000.

Example

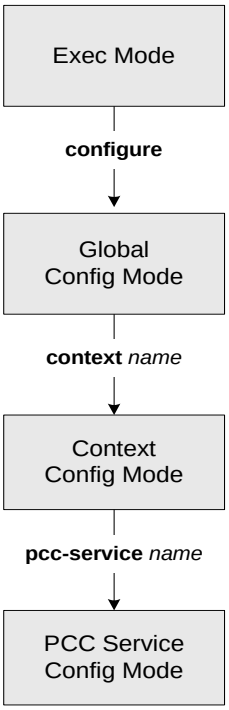
Following command sets the PCC-Service for handling of unknown services for PCC-Service-Profile instance on IPCF node to default action of **not allowed**:

```
default unknown-services-treatment
```

Chapter 223
PCC-Service Configuration Mode Commands

The PCC-Service Configuration Mode is used to link, consolidate and manage the policy logic for the network. It defines the authorization of resources for a subscriber's data usage under various conditions and policies in the PCC-service.

Important: This configuration mode is supported from StarOS Release 12.1 onward



action-set

This command is used to create a new set of action, action-set, or modify a previously configured action set and enters the PCC-Action-Set Configuration Mode. This command can also be used to delete an existing PCC-Action-Set.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

action-set *act_set_name* [**-noconfirm**]

no action-set *act_set_name*

no

Removes the configured PCC-Action-Set from this PCC-service instance for IPCF configuration.

act_set_name

Identifies the name of the PCC-Action-Set which is to be created or modified through this command.
The *act_set_name* must be an alphanumerical string from 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create/remove/configure an action-set in a PCC-service instance for IPCF Configuration.
An Action-set indicates the policy and charging as well as event generation related decisions that will get activated when the corresponding *Condition-Group* is evaluated to *TRUE* within a subscriber policy/profile.
A maximum of 512 PCC-Action-Sets can be configured in 1 instance of PCC-Service.
Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-action-set)
```

Important: For more information on PCC-Action-Set configuration, refer *PCC-Action-Set Configuration Mode Commands*.

Example

Following command creates a PCC-action-set named *pcc_act1* with in a PCC-service.

action-set *pcc_act1*

Following command removes a pre-configured PCC-action-set named *pcc_act1* from a PCC-service.

no action-set *pcc_act1*

charging method

This command defines the charging method selection parameters in a PCC-service instance for IPCF.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
charging method {both-offline-and-online | offline | online}

[default | no] charging method
```

default

Sets the charging method to "no" in a PCC-service instance on IPCF node.

no

Removes the configured charging method from a PCC-service instance on IPCF node.

both-offline-and-online

Default: Disabled.
Defines that this PCC-service instance is configured for both, online and offline, charging method for IPCF configuration.

offline

Default: Disabled.
Defines that this PCC-service instance is configured only for offline charging method for IPCF configuration.

online

Default: Disabled.
Defines that this PCC-service instance is configured only for online charging method for IPCF configuration.

Usage

Use this command to define the charging method selection parameters in a PCC-service instance for IPCF. Charging method used can be online, offline or both.

Example

Following command defines the charging method for a PCC-service instance as both, online and offline:

```
default charging method
```

charging server

This command defines the charging server parameters in a PCC-service instance for IPCF.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

charging server *server_name* **function** {**offline** | **online**} {**primary** | **secondary**}

no charging server {**all** | **function** {**offline** | **online**} {**primary** | **secondary**}

no

Removes/disables the charging server parameters in a PCC-service instance for IPCF configuration.

server_name

Identifies the name of the charging server which is to be configured with these parameters in a PCC-service instance for IPCF configuration.
The *server_name* must be an alphanumerical string from 1 through 63 characters.

offline

Sets the specific charging server to be used as offline server in a PCC-service instance for IPCF configuration.

online

Sets the specific charging server to be used as online server in a PCC-service instance for IPCF configuration.

primary

Sets the specific charging server to be used as primary charging server for offline or online charging method in a PCC-service instance for IPCF configuration.

secondary

Sets the specific charging server to be used as secondary charging server for offline or online charging method in a PCC-service instance for IPCF configuration.

all

This keyword is used with **no** keyword only. It removes the all configured charging server parameters from a PCC-service instance for IPCF configuration.

Usage

Use this command to configured the online or offline charging servers to be used as primary or secondary in a PCC-service instance for IPCF configuration.

Example

Following command configures the **online** charging server named *Gx1* as **primary** for online charging method for a PCC-service instance:

```
charging server Gx1 function online primary
```

Following command removes the all, online/offline/primary/secondary, type of charging servers from a PCC-service instance:

```
no charging server function all
```

condition-group

This command creates a new group of conditions, condition-group, or modify a previously configured condition-group and enters the PCC-Condition-Group Configuration Mode. This command can also be used to delete an existing PCC-Condition-Group.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

condition-group *cond_grp_name* [**-noconfirm**]

no condition-group *cond_grp_name*

no

Removes the configured PCC-condition-group from a PCC-service instance for IPCF configuration.

cond_grp_name

Identifies the name of the PCC-condition-group which is to be created or modified through this command. The *cond_grp_name* must be an alphanumerical string from 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create/remove/configure a group of condition, condition-group, in a PCC-service instance for IPCF configuration.
A Condition-group is a collection of conditions that identify a network or state constraint represented as an logical expression. A condition-group may use another **condition-group** within with the nesting level limited to 3.
Within a condition-group the conditions and condition-groups can either be linked with an **AND** or an **OR** relation. A Condition is built using predefined keywords representing unique service conditions such as *user-location*, *app-service* etc.
A maximum of 1024 PCC-Condition-Groups can be configured in 1 instance of PCC-Service.
Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-condition-group))#
```

The commands configured in this mode are defined in the *PCC-Condition-Group Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Caution: This is a critical configuration. The PCC-Condition Group can not be configured without this configuration. Any change to this configuration would lead to removing or disabling configuration parameters defined here.

Example

Following command creates a PCC-condition-group named *cond_grp1* with in a PCC-service instance.

```
condition-group cond_grp1
```

Following command removes a pre-configured PCC-condition-group named *cond_grp1* from a PCC-service instance.

```
no condition-group cond_grp1
```

data-service

This command creates a new service for data, data-service, or modify a pre-configured data-service and enters the PCC-Data-Service Configuration Mode. This command can also be used to delete an existing PCC-Data-Service.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

data-service *data_svc_name* [**-noconfirm**]

no data-service *data_svc_name*

no

Removes the configured PCC-Data-Service from a PCC-service instance for IPCF configuration.

data_svc_name

Identifies the name of the PCC-Data-Service which is to be created or modified through this command. The *data_svc_name* must be an alphanumerical string from 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create and configure a PCC-data-service in a PCC-service instance for IPCF configuration.
A PCC-Data-Service defines the flows for the media data as well as corresponding attributes that are necessary for the charging as well as policy enforcement decisions for the kind of media represented by its Service-Flows.
A maximum of 256 PCC-Data-Services can be configured in 1 instance of PCC-Service.
Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-data-service))#
```

The commands configured in this mode are defined in the *PCC-Data Service Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Caution: This is a critical configuration. The PCC-Data-service can not be configured without this configuration. Any change to this configuration would lead to removing or disabling configuration parameters defined here.

Example

Following command defines a PCC-data-service named *pcc_data_svc1* in a PCC-service instance without any confirmation prompt.

```
data-service pcc_data_svc1 -noconfirm
```

Following command removes a pre-configured PCC-data-service named *pcc_data_svc1* from a PCC-service instance without any confirmation prompt.

no data-service *pcc_data_svc1* **-noconfirm**

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

map-profile priority

This command defines the parameter and key priorities to match the profile condition for a subscriber in a PCC-service instance for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] map-profile priority map_prio_value  apn [apn_name profile-policy name
pcc_prof_name]

[no] map-profile priority map_prio_value profile-policy name pcc_prof_name]

[no] map-profile priority map_prio_value subscription-attribute name subs_attrib_name
[value] subs_attrib_value profile-policy name pcc_prof_name]
```

no

Removes/disables the set priority value of specific profile mapping parameters.

map_prio_value

Identifies the priority value of specific profile mapping parameters.
The *map_prio_value* must be an integer value from 1 through 1024.

apn *apn_name*

This keywords associates a pre-configured/defined APN name to map with specific profile mapping priority.
The *apn_name* specifies the name of the APN configured for subscriber session to which a priority value is set for profile mapping and must be an alphanumerical string from 1 through 63 characters.

condition-group *cond_grp_name*

This keywords associates a pre-configured/defined PCC-Condition-Group configured in PCC-Service Configuration mode to map with specific profile making priority.
The *cond_grp_name* is pre-configured PCC-Condition-Group and must be an alphanumerical string from 1 through 63 characters.

Important: For more information on PCC-Condition-Group configuration, refer **condition-group** command in this chapter.

spr-profile-not-found

This keyword set the condition based on unavailability of subscriber profile on SSC.
This support is provided to select a pre-configured profile policy *pcc_prof_name* if subscriber's SPR profile is not available and to allow operator to have different policies for such Subscribers.
If operator does not want to map a separate profile but treat such Subscribers differently, then a condition based on this criteria can be configured in *PCC-Condition-Group Configuration Mode*.

subscription-attribute name *subs_attrib_name*

This keywords associates a pre-configured/defined subscription attributes to map with specific profile making priority.
The *subs_attrib_name* specifies the subscription attribute name set/configured for the subscriber to which a priority value is set for profile mapping and must be an alphanumerical string from 1 through 63 characters.

value *subs_attrib_value*

This keywords associates a pre-configured/defined subscription attributes value associated with a subscription attribute name to map with specific profile making priority.
The *subs_attrib_value* specifies the subscription attribute value associated with a subscription attribute name set/configured for the subscriber to which a priority value is set for profile mapping and must be an alphanumerical string of 1 through 63 characters.

profile-policy *pcc_prof_name*

This keywords associates a pre-configured/defined PCC-Service-Profile configured in PCC-Service Configuration mode to map with specific profile making priority.
The *pcc_prof_name* is pre-configured PCC-Service-Profile and must be an alphanumerical string from 1 through 63 characters.

Important: For more information on PCC-Service-Profile configuration, refer **profile-policy** command in this chapter.

Usage

Use this command to identify the keys used to match the profile for a subscriber in a PCC-service instance for IPCF configuration.
The profile map is used when the subscriber session established. It is based on the priority of map and condition matches the corresponding named profile is used for the subscriber session.

Important: For a subscriber session, only a single profile will match.

Example

Following command configures the profile mapping priority to *2* for an APN named *apn_ipcf1* with PCC-Service-Profile named *pcc_prof1* with in a PCC-service instance.

```
map-profile priority 2 apn apn_ipcf1 profile-policy name pcc_profile1
```

Following command configures the profile mapping priority to *0* for all sessions with PCC-Service-Profile named *pcc_prof2* with in a PCC-service instance.

```
map-profile priority 2 profile-policy name pcc_profile2
```

monitoring-key

This command creates a monitoring key and sets the threshold to provide the facility for tracking and dynamic Policy control based on subscriber usage in a PCC-service instance for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

monitoring-key {**any** | *mon_key_value* **grant-size** *grant_volume*

[**no**]**monitoring-key** *mon_key_value*

[**default**] **monitoring-key any**

no

Removes/disables the configured Monitoring Key in IPCF.

any

Default: Enabled
This keywords sets the threshold size for ANY monitoring key to configured grant volume size. IPCF uses the configured grant size while installing a Monitoring Key in PCEF.

mon_key_value

This keywords configures the Monitoring Key with a configurable grant volume size. IPCF installs this Monitoring Key in PCEF for usage tracking.
mon_key_value must be an integer between 1 through 65535.

grant-size *grant_volume*

Default: 1024
This keywords associates a configurable grant size volume in Kilo Bytes for specific usage Monitor Key on IPCF to install on PCEF.
The *grant_volume* specifies the threshold volume in Kilo Bytes for any usage Monitoring Key and must be an integer between 1 through 4294967296.

Usage

Use this command to allow operator to configure the threshold size for a monitoring key in a PCC-service instance in IPCF. IPCF uses the configured grant size while installing a Monitoring Key in PCEF. The configured grant size value is configurable to reduce the amount of usage over shooting any of the usage conditions.
PCEF when instructed by IPCF keeps track of usage per Monitoring Key and also reports the usage when either thresholds reached or requested by IPCF.
To allow operator to have dynamic Policy control, the IPCF uses objects called as Usage Monitor. Currently an Usage Monitor has single attribute of Volume-limit only. Operator can “associate” different Monitoring

Keys to these usage monitors. It can be a Many-To-Many relationship between Usage-Monitor and Monitoring-Key.
Operator has option to set usage conditions on Usage Monitors instead of Monitoring Keys directly.

Example

Following command configures the Monitoring Key *2* for a grant size of *2048* Kilo Bytes with in a PCC-service instance.

```
monitoring-key 2 grant-size 2048
```

multiple-pcef-per-subscriber

This command enables the IPCF to support more than one **Gx**-session for single subscriber session coming from multiple PCEF in a PCC-service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no | default] multiple-pcef-per-subscriber
```

no

Default: Disabled
Removes the multiple **Gx** session for a single subscriber from a PCC-service instance for IPCF configuration.

default

Sets the PCC-service instance to default setting to accept the multiple **Gx** session for a single subscriber for IPCF configuration.

Usage

Use this command to enable multiple **Gx** session and multiple PCEF support for a single subscriber in a PCC-service instance for IPCF configuration.
By default this feature is enabled.

Example

Following command sets the IPCF to accept multiple **Gx** sessions from multiple PCEFs for a single subscriber with in a PCC-service instance.

```
multiple-pcef-per-subscriber
```

profile

This command creates a new PCC-Service-Profile or modifies a previously configured policy profile and enters the PCC-Service-Profile Configuration Mode. This command can also be used to delete an existing PCC-Service-Profile.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

profile *pcc_prof_name* [**-noconfirm**]

no profile *pcc_prof_name*

no

Removes the configured PCC-Service-Profile from a PCC-service instance for IPCF configuration.

pcc_prof_name

Identifies the name of the PCC-Service-Profile which is to be created or modified through this command. The *pcc_prof_name* must be an alphanumerical string from 1 through 63 characters. A maximum of 32 profiles can be configured in a PCC-service instance.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create/remove/configure a PCC-Service-Profile for managing the policy requirement and objectives for network specific to a group of subscribers in the network in a PCC-service instance for IPCF configuration.
A profile manages multiple *Condition-Groups* and associated *Action-Sets* pairs in an ordered manner. On internal or external triggers that cause the profile evaluation, the PCC-rules-engine, evaluates the conditions within the *Condition-Groups* in the specified priority. Corresponding actions performed for *Condition-Groups* that evaluates to *TRUE*. Once a *TRUE* match found the evaluation of *Condition-Groups* does not continue further.
A maximum of 32 PCC-Service-Profiles can be configured in 1 instance of PCC-Service.
Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-profile))#
```

The commands configured in this mode are defined in the *PCC-Service-Profile Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Caution: This is a critical configuration. The PCC-Service-Profile can not be configured without this configuration. Any change to this configuration would lead to removing or disabling configuration parameters defined here.

Example

Following command creates a PCC-Service-Profile named *pcc_prof1* with in a PCC-service instance.

```
profile pcc_prof1
```

Following command removes a pre-configured PCC-Service-Profile named *pcc_prof1* from a PCC-service instance.

```
no profile pcc_prof1
```

qos-profile

This command creates a new PCC-QoS-Profile for QoS parameters or modify a pre-configured PCC-QoS-Profile and enters the PCC-QoS-Profile Configuration Mode. This command can also be used to delete an existing PCC-QoS-Profile.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

qos-profile *qos_prof_name* [**-noconfirm**]

no qos-profile *qos_prof_name*

no

Removes the configured PCC-QoS-Profile from a PCC-service instance for IPCF configuration.

qos_prof_name

Identifies the name of the PCC-QoS-Profile which is to be created or modified through this command. The *qos_prof_name* must be an alphanumerical string from 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create and configure a PCC-QoS profile in a PCC-service instance for IPCF configuration.
A PCC-QoS-Profile represents a resource requirement identified by means of the corresponding QoS attributes such as:

- QoS class identifier
- Maximum Requested bandwidth for uplink (UL)
- Maximum Requested bandwidth downlink (DL)
- Guaranteed bandwidth for uplink (UL)
- Guaranteed bandwidth downlink (DL)
- Allocation and Retention Priority (ARP)

A maximum of 256 PCC-QoS-Profiles can be configured in 1 instance of PCC-Service.
Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-qos-profile))#
```

The commands configured in this mode are defined in the *PCC-QoS-Profile Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Caution: This is a critical configuration. The PCC-QoS-Profiles can not be configured without this configuration. Any change to this configuration would lead to removing or disabling configuration parameters defined here.

Example

Following command creates a PCC-QoS-Profile named *qos_profile1* with in a PCC-service instance.

```
qos-profile qos_profile1
```

Following command removes a pre-configured PCC-QoS-Profile named *qos_profile1* from a PCC-service instance.

```
no qos-profile qos_profile1
```

spr-failure

This command defines SSC session failure handling policies in a PCC-service instance on an IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
spr-failure after-auth {continue | terminate}

[default] spr-failure after-auth
```

default

Sets the configured SSC session failure handling parameters and actions to default action of **continue** with a PCC-service instance for IPCF configuration.

after-auth {continue | terminate}

This keyword is used to set the PCC-service to take decision on SSC communication failure after authorization of session.
Following actions are initiated on SSC session failure after authorization:

- **continue**: IPCF allows session to continue.
- **terminate**: IPCF terminates the session for subscriber.

Usage

Use this command to set the PCC-service to take decision on SSC communication failure after authorization of session.

Example

Following command sets the session failure handling policy with SSC to **terminate** the session on failure of communication with SSC after authorization in a PCC-service instance.

```
spr-failure after-auth terminate
```

ssc-usage-update-policy

This command provides the configuration to manage the SSC update frequency over **Sp** interface for usage reports received from PCEF over **Gx** interface in a PCC-service instance for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[default] ssc-usage-update-policy {always | average-tps tps | on-terminate}
```

default

Sets the PCC-service to configure the SSC update frequency to **always** over **Sp** interface for usage reports received from PCEF over **Gx** interface in a PCC-service instance for IPCF configuration.

always

Default: Enabled
This keyword sets the PCC-service instance to generate SSC usage update every time PCC-service instance received Usage Report from PCEF over **Gx** interface for IPCF configuration.

average-tps *tps*

Default: Disabled
This keyword generates the SSC usage update towards the SSC over **Sp** interface for Usage Reports received by IPCF from PCEF over **Gx** interface only when average transaction-per-second exceeds the configured threshold *tps*.
The *tps* specifies the average transactions-per-second on IPCF and must be an integer from 1 through 5000.

on-terminate

Default: Disabled
This keyword generates the SSC usage update towards the SSC over **Sp** interface for Usage Reports received by IPCF from PCEF over **Gx** interface only when IP-CAN session terminates.

Usage

Use this command to configure the PCC-service to manage the SSC update frequency over **Sp** interface for Usage Reports received from PCEF over **Gx** interface in a PCC-service instance for IPCF configuration.

Example

Following command configures the SSC usage update over **Sp** interface every time when a usage report is received over **Gx** interface in a PCC-service instance.

```
default ssc-usage-update-policy
```

timedef

This command creates a new Time Definition (TimeDef), or modify a pre-configured Timedef and enters the PCC-TimeDef Configuration Mode. This command can also be used to delete an existing PCC-TimeDef.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
[no] timedef timedef_name [-noconfirm]
```

no

Removes the configured PCC-TimeDef from a PCC-service instance for IPCF configuration.

timedef_name

Identifies the name of the PCC-TimeDef which is to be created or modified through this command.
The *timedef_name* must be an alphanumerical string from 1 through 127 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create and configure a PCC-Time Definition (TimeDef) in a PCC-service instance for IPCF configuration.
The PCC-TimeDefs can be used to configured date and time for triggering the event for policy related procedures as well.
Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-timedef))#
```

A maximum of 512 PCC-TimeDefs can be configured in 1 instance of PCC-Service.
The commands configured in this mode are defined in the *PCC-TimeDef Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Caution: This is a critical configuration. The PCC-TimeDefs can not be configured without this configuration. Any change to this configuration would lead to removing or disabling configuration parameters defined here.

Example

Following command creates a PCC-TimeDef named *time_day1* with in a PCC-service instance.

```
timedef time_day1
```

Following command removes a pre-configured PCC-TimeDef named *time_day1* from a PCC-service instance.

no timedef*time_day1*

timeout idle

Configures the idle timeout duration for subscriber session and also sets the action to be taken by system on expiry of timeout duration .

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

timeout idle *idle_dur* [**action reauthorize**]

no timeout idle

default timeout idle

no

Removes the configured idle timeout value and action set in in PCC Service instance.

default

Sets the the idle timeout duration to the default value of '0' which disables the idle timeout configuration in PCC Service instance.

idle_dur

Default: 0
Designates the maximum duration of the session, in seconds, after the expiry of which the system considers the session as dormant or idle and invokes the reauthorization of session action, if configured.
idle_dur must be a value in the range from 0 through 4294967295.
The special value 0 disables the timeout specified.

action reauthorize

This optional keyword sets the system to trigger the reauthorization of session after expiry of the timeout duration configured through *idle_dur* value.

Usage

Use this command to set the idle time duration for subscriber session to determine the dormant session.
This is configuration sets the time in seconds for idle session (sessions with no activity/signaling). On expiry of this timeout duration action of reauthorization of session shall be triggered. In case of reauthorization request failure, session termination shall be triggered.
Refer to the **timeout long-duration** command in this chapter for additional information.

Important: Reduce the timeout duration to free session resources faster for use by new requests.

Example

Following command sets the idle timeout duration to *450* seconds.

```
timeout idle 450
```

timeout setup

Configures the timeout duration for IPCF setup session.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

timeout setup *setup_dur*

no timeout setup

default timeout setup

no

Removes the configured setup timeout value and action set in in PCC Service instance.

default

Sets the the setup timeout duration to the default value of 60. The special value of '0' disables the setup timeout configuration in PCC Service instance.

setup_dur

Default: 60
Designates the maximum duration for the IPCF session setup, in seconds, after the expiry of which the system considers the IPCF session setup as failure and terminates the setup process.
setup_dur must be a value in the range from 0 through 120.
The special value 0 disables the setup timeout specified.

Usage

Use this command to set the time duration for IPCF session setup to determine the failure of IPCF setup process.

Example

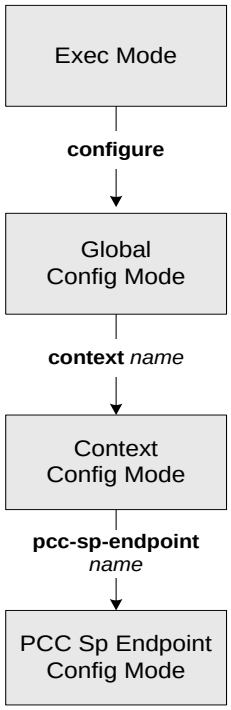
Following command sets the IPCF session timeout duration to *30* seconds.

```
timeout setup 30
```

Chapter 224
PCC-Sp-Endpoint Configuration Mode Commands

The PCC-Sp-Endpoint Configuration mode provides a mechanism for Intelligent Policy Control Function (IPCF) to support the **Sp** interface endpoint. It represents a client end for SSC interactions. The PCC-Sp-Endpoint configuration mode facilitates the configuration of **Sp** interface, and manages the connection and operational parameters related to its peer.

Important: This configuration mode is supported from StarOS Release 12.1 onward.



access-type

This command is used to define the type of access protocol to be used with a PCC-Sp-Endpoint instance for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
access-type {diameter | ldap}

default access-type
```

default

Sets access type protocol to be used by endpoints to default protocol of **Diameter** protocol in a PCC-Sp-Endpoint instance for IPCF configuration.

diameter

Default: Enabled
Sets access type protocol to be used by endpoints to Diameter protocol in a PCC-Sp-Endpoint instance for IPCF configuration.

ldap

Default: Disabled
Sets access type protocol to be used by endpoints to Lightweight Directory Access Protocol (LDAP) in a PCC-Sp-Endpoint instance for IPCF configuration.

Usage

Use this command to define the type of access protocol to be used with a PCC-Sp-Endpoint instance for IPCF configuration.

Example

Following command sets the access type of protocol to **Diameter** for a PCC-Sp-Endpoint instance.

```
default access-type
```

diameter dictionary

This command is used to assign a Diameter dictionary for interaction with SSC and messaging over **Sp** interface in a PCC-Sp-Endpoint instance of IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

diameter dictionary {**sh-custon-starent** | **sh-standard**}

default diameter dictionary

default

Sets the Diameter **Sh** dictionary to default dictionary **sh-custon-starent** (3GPP Rel. 8 Sh standard) for **Sh** interaction and messaging over **Sp** interface in a PCC-Sp-Endpoint instance of IPCF configuration.

sh-custom-starent

Default: Enabled
Sets the Diameter **Sh** dictionary to default dictionary **sh-custom-starent** for **Sh** interaction and messaging over **Sp** interface in a PCC-Sp-Endpoint instance of IPCF configuration.

sh-standard

Default: Disabled
Sets the Diameter **Sh** dictionary to default dictionary **sh-standard** (3GPP Rel. 8 standard) for **Sh** interaction and messaging over **Sp** interface in a PCC-Sp-Endpoint instance of IPCF configuration.

Usage

Use this command to assign a Diameter dictionary for **Sh** interaction and messaging over **Sp** interface in a PCC-Sp-Endpoint instance of IPCF configuration.

Example

Following command sets the Diameter dictionary for **Sh** interaction and messaging over **Sp** interface in a PCC-Sp-Endpoint instance of IPCF configuration to 3GPP Rel. 8 standard.

```
diameter dictionary sh-standard
```

diameter origin end-point

This command is used to bind/associate a pre-configured Diameter host/realm (SSC) over **Sp** interface for SPR interactions with a PCC-Sp-Endpoint instance to be used for subscriber profile and policy management.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

diameter origin endpoint *ssc_node_name*

no diameter origin endpoint

no

Removes the associated Diameter Origin Endpoint configuration from PCC-Sp-Endpoint instance configured for IPCF configuration.

ssc_node_name

The *ssc_node_name* is a predefined Diameter origin endpoint node (SSC) and must be an alphanumerical string from 1 through 63 characters.

Usage

Use this command to bind the SSC node over **Sp** interface by associating a pre-configured Diameter Origin Endpoint configuration with a PCC-Sp-Endpoint instance.
The Diameter origin endpoint must be a pre-configured instance in the Context Configuration Mode. For more information on Diameter origin endpoint configuration, refer *Diameter Endpoint Configuration Mode Commands* chapter.

Example

Following command associates a pre-configured Diameter endpoint node configuration named *ssc_1* with a PCC-Sp-Endpoint instance for subscriber policy profile management.

```
diameter origin endpoint ssc_1
```

Following command removes the pre-associated Diameter endpoint node configuration named *ssc_1* from a PCC-Sp-Endpoint instance.

```
no diameter origin endpoint
```

diameter peer-select

This command nominates primary and secondary Diameter peers amongst the peers configured under Diameter Endpoint Configuration instance which is associated with a PCC-Sp-Endpoint configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

diameter peer-select peer *pri_peer_name* [**realm** *realm_name*] [**secondary peer** *sec_peer_name* [**realm** *sec_realm_name*]]

no diameter peer-select

no

Removes the configured Diameter peer from peer-select process which are configured in Diameter Endpoint configuration associated with PCC-Sp-Endpoint instance configured for IPCF configuration.

peer *pri_peer_name*

Sets a configured Diameter peer, which is configured in Diameter Endpoint configuration associated with PCC-Sp-Endpoint instance configuration, as **primary** in Diameter peer selection process for IPCF configuration.
The *pri_peer_name* is a pre-configured Diameter peer in Diameter Endpoint configuration which is associated with a PCC-Sp-Endpoint configuration and must be an alphanumerical string from 1 through 63 characters. *pri_peer_name* allows punctuation marks.

realm *realm-name*

This keyword optionally defines the realm (domain) of a configured **primary** Diameter peer, which is configured in Diameter Endpoint configuration associated with PCC-Sp-Endpoint instance configuration, in Diameter peer selection process for IPCF configuration.
realm_name is the realm (domain) of the associated primary Diameter peer in Diameter Endpoint configuration which associated with a PCC-Sp-Endpoint configuration. The *realm_name* must be an alpha and/or numeric string of from 1 to 127 characters. The realm may typically be a company or service name and it allows punctuation marks.

secondary peer *sec_peer_name*

Sets a configured Diameter peer, which is configured in Diameter Endpoint configuration associated with PCC-Sp-Endpoint instance configuration, as **secondary** in Diameter peer selection process for IPCF configuration.
The *sec_peer_name* is a pre-configured Diameter peer in Diameter Endpoint configuration which is associated with a PCC-Sp-Endpoint configuration and must be an alphanumerical string from 1 through 63 characters. *sec_peer_name* allows punctuation marks.

realm *sec_realm-name*

This keyword optionally defines the realm (domain) of a configured **secondary** Diameter peer, which is configured in Diameter Endpoint configuration associated with PCC-Sp-Endpoint instance configuration, in Diameter peer selection process for IPCF configuration.
sec_realm_name is the realm (domain) of the associated primary Diameter peer in Diameter Endpoint configuration which associated with a PCC-Sp-Endpoint configuration. The *sec_realm_name* must be an alpha and/or numeric string of from 1 to 127 characters. The realm may typically be a company or service name and it allows punctuation marks.

Usage

Use this command to nominate primary and secondary Diameter peers amongst the peers configured under Diameter Endpoint Configuration instance which is associated with a PCC-Sp-Endpoint configuration. When both primary and secondary are down, the remaining Diameter peers are chosen based on their configured weight in round robin manner.
Multiple Diameter peers can be configured in a PCC-Sp-Endpoint instance by entering this command multiple times.

Example

Following command nominates a pre-configured Diameter peer *dia1* as primary and *dia2* as secondary for Diameter peer selection process in a PCC-Sp-Endpoint configuration instance.

```
diameter peer-select peer dia1 secondary peer dia2
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

profile-data

This command allows the operator to specify data-reference and service indication AVP values used in UDR/SNR message for profile data sent over **Sp** endpoint when access type is set to Diameter.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

profile-data key data-reference *data_ref_value* [**service-indication** *svc_ind_value*]

default profile-data key

default

Specifies the data-reference value used in UDR/SNR message for profile data sent over **Sp** endpoint to default value of '*0*' (zero) and service indication AVP value to *profile data* when access type is set to Diameter in PCC-Sp-Endpoint instance.

data-reference *data_ref_value*

Default: 0
Specifies the data-reference values used in UDR/SNR message for profile data sent over **Sp** endpoint when access type is set to Diameter in PCC-Sp-Endpoint instance.
The data reference value *data_ref_value* must be an integer from 1 through 65535.

service-indication *svc_ind_value*

Specifies the service indication AVP value used in UDR/SNR message for profile data sent over **Sp** endpoint when access type is set to Diameter in PCC-Sp-Endpoint instance.

Important: The Service-Indication values are set as per application logic and are supposed to be used only with SSC.

The service indication value *svc_ind_value* must be a string of alpha and/or numeric characters from 1 to 32 characters.

Usage

Use this command to allow the operator to specify data-reference and service indication AVP values used in UDR/SNR message for profile data sent over **Sp** endpoint when access type is set to Diameter in PCC-Sp-Endpoint configuration instance.
Default service-indication value varies as per other interface configuration **default profile-data key** is used to set the service indication value.

Example

Following command set the data-reference value used in UDR/SNR message for profile data sent over **Sp** endpoint to default value of '*0*' (zero) and service-indication value as per application logic when access type is set to Diameter in PCC-Sp-Endpoint instance.

```
default profile-data key
```

profile-update-notification

This command sets the system to indicate whether SSC and IPCF are capable of supporting profile update notifications in a PCC-Sp-Endpoint instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

```
profile-update-notification {allow | disallow}

default profile-update-notification
```

default

Set the PCC-Sp-Endpoint instance default mode for supporting profile update notifications in a PCC-Sp-Endpoint instance and also to use the same in a PCC-Sp-Endpoint configuration instance.

allow

Default: Enabled
Set the PCC-Sp-Endpoint instance to support the profile update notifications and also allow to use the same in **Sp** interaction.

disallow

Default: Disabled
Set the PCC-Sp-Endpoint instance to not to support the profile update notifications and also does not allow to use the same in **Sp** interaction.

Usage

Use command to set to indicate whether SSC and IPCF are capable of supporting profile update notifications in a PCC-Sp-Endpoint instance. It also sets that whether profile update notification should be used or not for a PCC-Sp-Endpoint configuration instance.

Example

Following command indicates that SSC and IPCF are capable of supporting profile update notifications in a PCC-Sp-Endpoint instance and also allow to use it for a PCC-Sp-Endpoint configuration instance.

```
default profile-update-notification
```

spr subscriber identifier

This command sets the PCC-Sp-Endpoint instance to indicate how a subscriber is uniquely identified in SPR database while requesting subscriber data from SSC.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

spr subscriber identifier {**imsi** | **msisdn** | **nai**}

default spr subscriber identifier

default

Sets the PCC-Sp-Endpoint instance to use subscriber IMSI to identify subscriber uniquely in SPR database while requesting subscriber data from SSC.

imsi

Default: Enabled
Sets the PCC-Sp-Endpoint instance to use subscriber IMSI to identify subscriber uniquely in SPR database while requesting subscriber data from SSC.

msisdn

Default: Disabled
Sets the PCC-Sp-Endpoint instance to use subscriber MSISDN to identify subscriber uniquely in SPR database while requesting subscriber data from SSC.

nai

Default: Disabled
Sets the PCC-Sp-Endpoint instance to use Network Address Identifier as token to identify subscriber uniquely in SPR database while requesting subscriber data from SSC.
This token facilitates CDMA users for Policy Control and Charging functions.

Usage

Use command to set the PCC-Sp-Endpoint instance to indicate how a subscriber is uniquely identified in SPR database on SSC while requesting subscriber data. By default it uses Subscriber IMSI for identification in SPR database.
For IP-CAN session between PDSN and IPCF the subscriber token NAI facilitates the Policy Control and Charging functions to subscribers.

Example

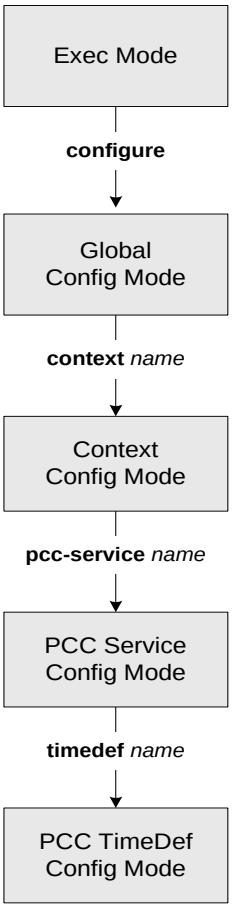
Following command sets the PCC-Sp-Endpoint instance to use a subscriber IMSI to uniquely identified in SPR database at SSC.

```
default spr subscriber identifier
```

Chapter 225
PCC-TimeDef Configuration Mode Commands

The PCC-TimeDef Configuration Mode is used to configure various time definitions (TimeDefs) in the PCC-service instance. A PCC-TimeDef specifies the start and end time for triggering policy-related procedures or conditions.

Important: This configuration mode is supported from StarOS Release 12.1 onward.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

start date

This command defines PCC-TimeDefs with a start and end dates with time for an event to trigger a procedure or condition in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] start date *start_date* **time** *start_time* **end date** *end_date* **time** *end_time*

no

Removes the specified time definition.

date *start_date*

Specifies the start date *start_date* in *MM*/*DD*/*YY* format.
Following format is used for *MM*/*DD*/*YY* in *start_date*:

- *MM* specifies the month of the start date from January through December and must be an integer between 1 through 12.
- *DD* specifies the date of month of the start date 1 through 31 and must be an integer between 1 through 31.
- *YY* specifies the year of the start date from 2010 through 2037 and must be an integer between 10 through 37.

time *start_time*

Specifies the start time *start_time* in *HH MIN SS* format.
Following format is used for *HH MIN SS* in *start_time*:

- *HH* specifies the hour of the start date in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the start date must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the start date must be an integer between 00 through 59.

end date *end_date*

Specifies the end date *end_date* in *MM*/*DD*/*YY* format.
Following format is used for *MM*/*DD*/*YY* in *end_date*:

- *MM* specifies the month of the end date from January through December and must be an integer between 1 through 12.
- *DD* specifies the date of month of the end date 1 through 31 and must be an integer between 1 through 31.
- *YY* specifies the year of the end date from 2010 through 2037 and must be an integer between 10 through 37.

time *end_time*

Specifies the end time *end_time* in *HH MIN SS* format.
Following format is used for *HH MIN SS* in *end_time*:

- *HH* specifies the hour of the end date in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the end date must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the end date must be an integer between 00 through 59.

Usage

Use this command to define a PCC-TimeDef with a start and end dates with time for an event to trigger a procedure or condition in an IP-CAN session.

Example

The following command defines a PCC-TimeDef with start date as December 31st 2010 at 00 Hrs. 30 mins. and 00 seconds and end date as January 31st 2011 at 23 Hrs. 59 mins. and 59 seconds:

start date *12/31/10* **time** *00 30 00* **end date** *01/31/11* **time** *23 59 59*

start day

This command defines PCC-TimeDefs with a start and end week days with time for an event to trigger a procedure or condition in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] start day *start_weekdays* **time** *start_time* **end day** *end_weekdays* **time** *end_time*

no

Removes the specified time definition.

day *start_weekdays*

Specifies the start day as week days.
Following days are used as *start_weekdays*:

- **friday** specifies Friday of the week as start day.
- **monday** specifies Monday of the week as start day.
- **saturday** specifies Saturday of the week as start day.
- **sunday** specifies Sunday of the week as start day.
- **thrusday** specifies Thursday of the week as start day.
- **tuesday** specifies Tuesday of the week as start day.
- **wednesday** specifies Wednesday of the week as start day.

time *start_time*

Specifies the start time *start_time* in *HH MIN SS* format.
Following format is used for *HH MIN SS* in *start_time*:

- *HH* specifies the hour of the start day in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the start day must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the start day must be an integer between 00 through 59.

end day *end_weekdays*

Specifies the end day as week days.
Following days are used as *end_weekdays*:

- **friday** specifies Friday of the week as end day.
- **monday** specifies Monday of the week as end day.
- **saturday** specifies Saturday of the week as end day.

- **sunday** specifies Sunday of the week as end day.
- **thrusday** specifies Thursday of the week as end day.
- **tuesday** specifies Tuesday of the week as end day.
- **wednesday** specifies Wednesday of the week as end day.

time *end_time*

Specifies the end time *end_time* in *HH MIN SS* format.
Following format is used for *HH MIN SS* in *end_time*:

- *HH* specifies the hour of the end day in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the end day must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the end day must be an integer between 00 through 59.

Usage

Use this command to define a PCC-TimeDef with a start and end weekdays with time for an event to trigger a procedure or condition in an IP-CAN session.

Example

The following command defines a PCC-TimeDef with start day as Friday at 00 Hrs. 30 mins. and 00 seconds and end day as Sunday at 23 Hrs. 59 mins. and 59 seconds:

```
start day friday time 00 30 00 end day sunday time 23 59 59
```

start time

This command defines PCC-TimeDefs with a start and end time of a day for an event to trigger a procedure or condition in an IP-CAN session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[no] start time start_time end time end_time
```

no

Removes the specified time definition.

time *start_time*

Specifies the start time *start_time* in *HH MIN SS* format.
Following format is used for *HH MIN SS* in *start_time*:

- *HH* specifies the hour of the day in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the day must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the day must be an integer between 00 through 59.

end time *end_time*

Specifies the end time *end_time* in *HH MIN SS* format.
Following format is used for *HH MIN SS* in *end_time*:

- *HH* specifies the end hour of the day in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the end hour of the day must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the end hour must be an integer between 00 through 59.

Usage

Use this command to define a PCC-TimeDef with a start and end time for an event to trigger a procedure or condition in an IP-CAN session.

Example

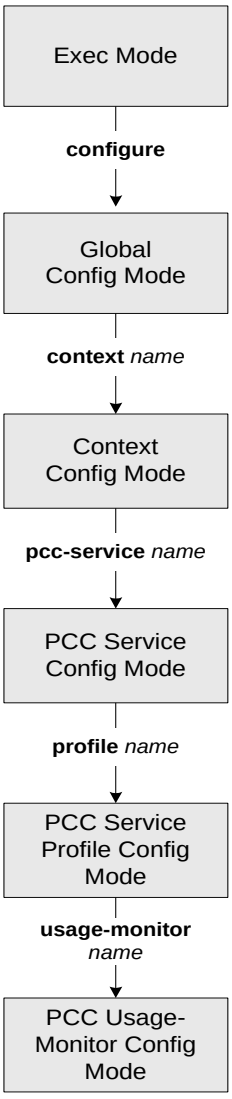
The following command defines a PCC-TimeDef with start at 00 Hrs. 30 mins. and 00 seconds and end at 23 Hrs. 59 mins. and 59 seconds:

```
start time 00 30 00 end time 23 59 59
```

Chapter 226
PCC-Usage-Monitor Configuration Mode Commands

The PCC-Usage-Monitor Configuration mode provides a mechanism to set the usage threshold limit in a PCC-Service-Profile to trigger a required condition and action set in PCC-Service instance.

Important: This configuration mode is supported from StarOS Release 12.1 onward.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

usage-limit volume

Sets the usage limit by volume for a subscriber profile for a PCC-Service-Profile on an IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Syntax

[**default usage-limit volume** [**downlink** *dlink_volume* | **total** *total_volume* | **uplink** *uplink_volume*]

default

Sets the usage limit volume to "0" for downlink, uplink and total bucket in a PCC-Service-Profile.

downlink *dlink_volume*

Specifies the usage volume (in kilobytes) in the downlink direction (from PCEF to UE) as an integer from 1 through 4294967296. A "0" (zero) value disables the downlink volume usage. Default: 0

total *total_volume*

Specifies the usage volume (in kilobytes) in the downlink and uplink directions (from PCEF to UE and PCEF to PDN) as an integer from 1 through 4294967296. A "0" (zero) value disables the downlink volume usage. Default: 0

uplink *uplink_volume*

Specifies the usage volume (in kilobytes) in the uplink direction (from PCEF to PDN) as an integer from 1 through 4294967296. A "0" (zero) value disables the downlink volume usage. Default: 0

Usage

Use this command to set the usage limit in volume for subscriber profile for a PCC-Service-Profile on IPCF node.

Example

The following command sets the usage limit volume to 20000 kilobytes in the upload direction within a PCC-Service-Profile.

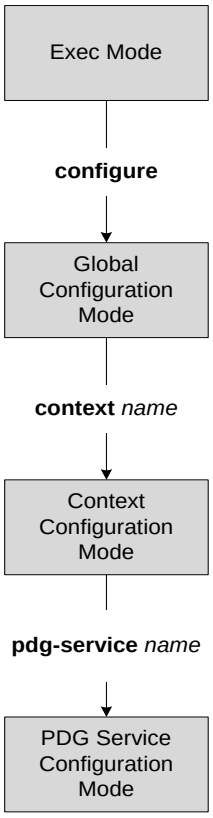
```
usage-limit volume uplink 20000
```

The following command sets the usage limit volume to 400000 kilobytes in the download direction within a PCC-Service-Profile.

```
usage-limit volume downlink 400000
```

Chapter 227
PDG Service Configuration Mode Commands

The PDG Service Configuration Mode is used to specify the properties required for the UEs in the WLAN (Wireless Local Access Network) to interface with the Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG).



aaa attribute

Sets the attributes that the system uses in AAA messages.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

```
aaa attribute { 3gpp-negotiated-qos-profile string }

no aaa attribute
```

3gpp-negotiated-qos-profile *string*

Specifies the 3GPP negotiated QoS profile to use in AAA messages during IMS emergency call handling as an alphanumeric string of 1 through 31 characters.

no aaa attribute

Removes a previously configured AAA attribute.

Usage

Specifies the 3GPP negotiated QoS profile to use in AAA messages during IMS emergency call handling.

Example

The following command specifies the 3GPP negotiated QoS profile to use during IMS emergency call handling:

```
aaa attribute 3gpp-negotiated-qos-profile 100
```

associate sgtp-service

Identifies the SGTP service to be associated with the PDG service to enable TTG functionality on the PDG/TTG. TTG functionality supports GTP-C (GTP control plane) messaging and GTP-U (GTP user data plane) messaging between the TTG and the GGSN over the Gn' interface.

Important: This command can be used before the associated service instance is created and configured but care should be used to match the service names.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

`[ no ] associate sgtp-service` *`sgtp_service_name`* **`[ context`** *`sgtp_context_name`* **`]`**

`no`

Removes the service association definition from the configuration.

`sgtp-service` *`sgtp_service_name`*

Specifies which SGTP service configuration, by naming the SGTP service instance, to associate with this PDG service.
`sgtp_service_name` is an alphanumeric string of 1 through 63 characters with no spaces.

`context` *`sgpt_context_name`*

Defines the context in which the SGTP service was created. If no context is specified, the current context is used.
`sgtp_context_name` is an alphanumeric string of 1 through 63 characters with no spaces.

Usage

Use this command to associate the SGTP service to be associated with the PDG service to enable TTG functionality on the PDG/TTG.

Example

The following command associates SGTP service *`sgtp_service_1`* with this PDG service:

```
associate sgtp-service sgtp_service_1 context sgtp_context_1
```

certificate-selection

Configures the PDG/TTG to select the trusted certificate (and the private key for calculating the AUTH payload) to be included in the first IKE_AUTH message from the PDG/TTG based on the APN (Access Point Name). The selected certificate is associated with the APN included in the IDr payload of the first IKE_AUTH message from the UE.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] certificate-selection apn-based

default certificate-selection
```

certificate-selection apn-based

Selects a trusted certificate for the first IKE-AUTH message based on the APN.

no certificate-selection

Disables APN-based certificate selection and resumes sending a certificate bound to a crypto template.

default certificate-selection

Sets the default certificate selection method to a certificate bound to a crypto template.

Usage

Configures the PDG/TTG to select the trusted certificate to be included in the first IKE_AUTH message based on the APN.

Example

Use the following example to enable APN-based certificate selection:

```
certificate-selection apn-based
```

bind

Binds the PDG service IP address to a crypto template and specifies the maximum number of sessions the PDG service supports.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

`[ no ] bind address` *`ipv4_address`* **`{ crypto-template`** *`string`* **`} mode { ttg | pdg } [ max-sessions`** *`number`* **`]`**

`no`

Removes a previously configured binding.

`bind address` *`ipv4_address`*

Specifies the IPv4 address of the PDG service with which the UE attempts to establish an IKEv2/IPSec tunnel. This address must be a valid IP address within the context.
This is a mandatory parameter.

`crypto-template` *`string`*

Specifies the name of the crypto template to be bound to the PDG service. This is the name of the IPSec policy to be used as a template for PDG/TTG subscriber session IPSec policies. The crypto template includes most of the IPSec and IKEv2 parameters for keepalive, lifetime, NAT-T, and cryptographic and authentication algorithms. There must be one crypto template per PDG service.
This is a mandatory parameter.
`string` is an alphanumeric string of 0 through 127 characters.

`mode { ttg | pdg }`

Default: There is no default value.
Specifies whether the PDG service provides TTG or PDG functionality, as follows:

- In TTG mode, PDN connectivity is provided through the GGSN. PDG functionality is provided by the combined TTG and GGSN.
- In PDG mode, PDN connectivity and PDG functionality are provided directly through the PDG service.

This is a mandatory parameter.

Important: PDG mode is not supported in this software release.

Dependencies:
When you configure the PDG service to be in TTG mode, you must also configure the SGTP service using the **`associate sgtp-service`** command, as the TTG needs to connect with the GGSN to complete the PDG functionality.
The following behaviors occur when the PDG service operates in TTG mode:

- If the SGTP service associated with PDG service is not configured, the PDG service is not started.

- If the SGTP service associated with PDG service is not started, the PDG service is not started.
- If the SGTP service associated with PDG service is stopped, the PDG service is stopped.
- If the SGTP service associated with PDG service is re-started, the PDG service is re-started.
- If the SGTP service is not yet configured, whenever the SGTP service is started, the PDG service is started.

Note that starting or stopping the PDG service has no impact on the SGTP service.

---

max-sessions *number*

Specifies the maximum number of sessions to be supported by the PDG service as an integer from 0 through 1000000. Default: 1000000
If the max-sessions value is changed on an existing system, the new value takes effect immediately if it is higher than the current value. If the new value is lower than the current value, existing sessions remain established, but no new sessions are permitted until usage falls below the newly-configured value.

Usage

Use this command in PDG Service Configuration Mode to bind the IP address used as the connection point for establishing IKEv2/IPSec sessions to a crypto template. You can also use it to define the maximum number of sessions the PDG service supports.

Example

The following command binds a PDG service with an IP address of *10.2.3.4* to the crypto template *crypto_template_1*, sets the mode to TTG, and sets the maximum number of sessions to *500000*:

```
bind address 10.2.3.4 crypto-template crypto_template_1 mode ttg max-
sessions 500000
```

ip gnp-qos-dscp

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets over the Gn' interface in the uplink direction.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

`[ no ] ip gnp-qos-dscp {  background` *`dscp`* **`| conversational`***`dscp`* **`| interactive`** *`dscp`* **`| streaming`** *`dscp`* **`| interactive [ traffic-handling-priority`** *`traffic_priority`* **`] { allocation-retention-priority`** *`allocation_retention_priority`* **`} } +`**

`default ip gnp-qos-dscp`

`no`

Disables the overriding of the ToS (Type of Service) field and enables the pass-through option.

`background` *`dscp`*

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP background class, in which the data transfer is not time-critical (for example, in e-mail exchanges). This traffic class is the lowest QoS.
`dscp`: Sets the DSCP for the specified traffic class. See the *`dscp`* section below.

`conversational` *`dscp`*

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP conversational class, in which there is a constant flow of traffic in both the uplink and downlink direction. This traffic class is the highest QoS.
`dscp`: Sets the DSCP for the specified traffic pattern. See the dscp section below.

`interactive [ traffic-handling-priority` *`traffic_priority`* **`]`**

Specifies the DSCP marking to be used for packets of sessions subscribed to three possible traffic priorities in the 3GPP interactive class, in which there is an intermittent flow of packets in the uplink and downlink direction. This traffic class has a higher QoS than the background class, but not as high as the streaming class.
`traffic_priority` is the 3GPP traffic handling priority and can be the integers 1, 2 or 3.

`allocation-retention-priority` *`allocation_retention_priority`*

Specifies the DSCP for the interactive class if the allocation priority is present in the QoS profile.
`allocation-retention-priority` can be the integers 1, 2, or 3.
DSCP uses the values in the following table based on the traffic handling priority and allocation/retention priority if the allocation priority is present in the QOS profile.

Allocation Priority	1	2	3
Traffic Handling Priority			
1	ef	ef	ef

Allocation Priority	1	2	3
2	af21	af21	af21
3	af21	af21	af21

Important: If you only configure DCSP marking for interactive traffic classes without specifying ARP, it may not properly take effect. The CLI allows this scenario for backward compatibility however, it is recommended that you configure all three values.

`streaming` *`dscp`*

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP streaming class, in which there is a constant flow of data in either in the uplink or downlink direction. This traffic class has a higher QoS than the interactive class, but not as high as the conversational class.
dscp: Set the DSCP for the specified traffic pattern. See the dscp section below.

`dscp`

Default:

- background: be
- interactive
- Traffic Priority 1: ef
- Traffic Priority 1: af21
- Traffic Priority 1: af21
- streaming: af11
- conversational: ef

Specifies the DSCP for the specified traffic pattern. *`dscp`* can be configured to any one of the following:

• af11: Assured Forwarding 11 per-hop-behavior (PHB)	• af33: Assured Forwarding 33 PHB
• af12: Assured Forwarding 12 PHB	• af41: Assured Forwarding 41 PHB
• af13: Assured Forwarding 13 PHB	• af42: Assured Forwarding 42 PHB
• af21: Assured Forwarding 21 PHB	• af43: Assured Forwarding 43 PHB
• af22: Assured Forwarding 22 PHB	• be: Best effort forwarding PHB
• af23: Assured Forwarding 23 PHB	• ef: Expedited forwarding PHB
• af31: Assured Forwarding 31 PHB	

• af32: Assured Forwarding 32 PHB	

+

More than one of the above keywords can be entered within a single command.

Usage

DSCP levels can be assigned to specific traffic patterns in order to ensure that data packets are delivered according to the precedence with which they're tagged. The diffserv markings are applied to the IP header of every subscriber data packet transmitted over the Gn' interface(s).
The four traffic patterns have the following order of precedence: background (lowest), interactive, streaming, and conversational (highest). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in the following tables:

Drop Precedence	Class			
	Class 1	Class 2	Class 3	Class 4
Low	af11	af21	af31	af41
Medium	af12	af22	af32	af41
High	af13	af23	af33	af43

Precedence (low to high)	DSCP
1	Best Effort (be)
2	Class 1
3	Class 2
4	Class 3
5	Class 4
6	Express Forwarding (ef)

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

Example

The following command configures the DSCP level for the streaming traffic pattern to be ef:**`ip gnp-qos-dscp streaming ef`**
The following command configures the DSCP levels for the conversational, streaming, interactive and background traffic patterns to be ef, af22, and af41, respectively:**`ip gnp-qos-dscp conversational ef streaming ef interactive af22 background af41`**

ip qos-dscp

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets over the Wu interface in the downlink direction.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

ip qos-dscp { **qci** { **1** { *dscp-pt* } | **2** { *dscp-pt* } | **3** { *dscp-pt* } | **4** { *dscp-pt* } | **5** { *allocation-retention-priority 1..3* | *dscp-pt* } | **6** { *allocation-retention-priority 1..3* | *dscp-pt* } | **7** { *allocation-retention-priority 1..3dscp* | *dscp-pt* } | **8** { *allocation-retention-priority 1..3* | *dscp-pt* } | **9** { *dscp-pt* } *+* }

no ip qos-dscp { **qci** { 1 | 2 | 3 | 4 | 5 { *allocation-retention-priority 1..3* | *dscp-pt* } | 6 { *allocation-retention-priority 1..3* | *dscp-pt* } | 7 { *allocation-retention-priority 1..3* | *dscp-pt* } | 8 { *allocation-retention-priority 1..3* | *dscp-pt* } | 9 {*+*

allocation-retention-priority

Specifies the DSCP for interactive class if the allocation priority is present in the QOS profile.
allocation-retention-priority can be the integers 1, 2, or 3.
DSCP values use the following matrix to map based on traffic handling priority and Alloc/Retention priority if the allocation priority is present in the QOS profile.
The following table shows the DSCP value matrix for *allocation-retention-priority*.

Table 29. Default DSCP Value Matrix

	Allocation Priority 1	Allocation Priority 2	Allocation Priority 3
Traffic Handling Priority			
1	ef	ef	ef
2	af21	af21	af21
3	af21	af21	af21

qci

Configures the QCI attribute of QoS. Here the *qci_val* is the QCI for which the negotiate limit is being set, it ranges from 1 to 9.

dscp

Default QCI:
- 1: ef

- 2: ef
- 3: af11
- 4: af11
- 5: ef
- 6: ef
- 7: af21
- 8: af21
- 9: be

Specifies the DSCP for the specified traffic pattern. *dscp* can be configured to any one of the following:

• **af11:** Assured Forwarding 11 per-hop-behavior (PHB)	• **af32:** Assured Forwarding 32 PHB
• **af12:** Assured Forwarding 12 PHB	• **af33:** Assured Forwarding 33 PHB
• **af13:** Assured Forwarding 13 PHB	• **af41:** Assured Forwarding 41 PHB
• **af21:** Assured Forwarding 21 PHB	• **af42:** Assured Forwarding 42 PHB
• **af22:** Assured Forwarding 22 PHB	• **af43:** Assured Forwarding 43 PHB
• **af23:** Assured Forwarding 23 PHB	• **be:** Best effort forwarding PHB
• **af31:** Assured Forwarding 31 PHB	• **ef:** Expedited forwarding PHB

+

More than one of the above keywords can be entered within a single command.

Usage

You can assign DSCP to specific traffic patterns to ensure that data packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the outer IP header of every GTP data packet. The diffserv marking of the inner IP header is not modified.
The traffic patterns are defined by QCI (1 to 9). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in the following tables:

Table 30. Class structure for assured forwarding (af) levels

Drop Precedence	Class			
	Class 1	Class 2	Class 3	Class 4
Low	af11	af21	af31	af41
Medium	af12	af22	af32	af41
High	af13	af23	af33	af43

Table 31. DSCP Precedence

Precedence (low to high)	DSCP
0	Best Effort (be)
1	Class 1
2	Class 2
3	Class 3
4	Class 4
5	Express Forwarding (ef)

The DSCP level can be configured for multiple traffic patterns within a single instance of this command. The no ip qos command can be issued to remove a QOS setting and return it to it's default setting.

Example

The following command configures the DSCP level for QCI to be Expedited Forwarding,**ef**:

```
ip qos-dscp qci 1 ef
```

ip source-violation

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected, or for verifying packet routing and labeling within the network.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

ip source-violation { clear-on-valid-packet | drop-limit *num* **period** *secs* **}**

default ip source-violation { drop-limit *num* **period** *secs* **}**

no ip source-violation clear-on-valid-packet

clear-on-valid-packet

Configures the service to reset the drop-limit counters upon receipt of a properly addressed packet. Default: disabled

drop-limit *num*

Sets the maximum number of allowed IP source violations within the detection period before dropping a call. If *num* is not specified, the value is set to the default value.
num is an integer from 1 to 1000000. Default: 10

period *secs*

Sets the detection period (in seconds) for IP source violations as an integer from 1 through 1000000. If *secs* is not specified, the value is set to the default value. Default: 120

default ip source-violation { drop-limit *num* **period** *secs* **}**

Sets or restores the IP source violation detection defaults, as follows:

- **drop-limit**: Sets or restores the maximum number of IP source violations within the detection period before dropping the call to the default value of 10.
- **period**: Sets or restores the detection period for IP source violations to the default value of 120 seconds.

no ip source-violation clear-on-valid-packet

The drop-limit counters are not reset upon receipt of a properly addressed packet.

Usage

Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.
Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

This function operates in the following manner: When a subscriber packet is received with a source IP address violation, the system increments the IP source violation drop-limit counter and starts the timer for the IP source violation period. Every subsequent packet received with a bad source address during the IP source violation period causes the drop-limit counter to increment. For example, if the drop-limit is set to 10, after 10 source violations, the call is dropped. The detection period timer continues to count throughout this process.

Example

The following command sets the drop limit to 15 and leaves the other values at their default values:

```
ip source-violation drop-limit 15
```

max-tunnels-per-ue

Specifies the maximum number of IKEv2/IPSec tunnels allowed per UE by the PDG/TTG. This maximum number is specified per PDG service.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

max-tunnels-per-ue *integer*

default max-tunnels-per-ue

integer

Specifies the maximum number of IKEv2/IPSec tunnels allowed per UE as an integer from 1 to 11. Default: 11

default max-tunnels-per-ue

Sets the maximum number of IKEv2/IPSec tunnels allowed per UE to its default value, which is 11.

Usage

Use this command to set the maximum number of IKEv2/IPSec tunnels allowed per UE.

Example

Use the following command to set the maximum number of IKEv2/IPSec tunnels allowed per UE to *2*:

```
max-tunnels-per-ue 2
```

plmn id

Configures location specific mobile network identifiers used to help translate local emergency and service-related numbers. Default is disabled.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

plmn id mcc *mcc_number* **mnc** *mnc_number*

no plmn id mcc *mcc_number* **mnc** *mnc_number*

---

mcc *mnc_number*

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 200 through 999.

---

mnc *mnc_number*

Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 2-digit integer from 00 through 999.

---

no plmn id mcc *mcc_number* **mnc** *mnc_number*

Removes a previously configured PLMN identifier for the PDG service.

Usage

The PLMN ID is included in the RAI (Routing Area Identity) field of the PDP Create Request messages sent to the GGSN. Multiple PDG services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each PDG service.

Example

The following command configures the PLMN identifier with an MCC of *462* and MNC of *2*:

```
plmn id mcc 462 mnc 02
```

setup-timeout

Specifies the maximum time allowed to set up a session.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

setup-timeout *integer*

default setup-timeout

setup-timeout integer

Sets the session setup timeout value (in seconds) as an integer from 2 through 300. Default: 60

default setup-timeout

Sets or restores the default session setup timer value to 60 seconds.

Usage

The PDG/TTG clears both the user session and tunnels if a call does not initiate successfully before the session setup timer expires.

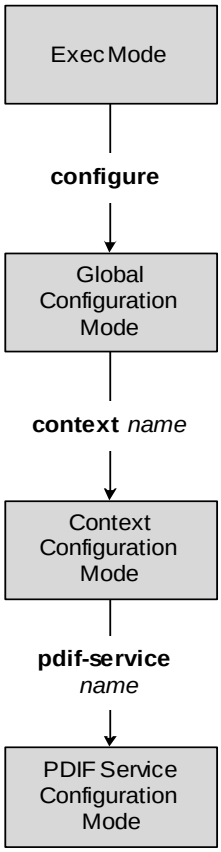
Example

The following command sets the session setup timeout value to the default value of 60 seconds:

```
default setup-timeout
```

Chapter 228
PDIF Service Configuration Mode Commands

The PDIF Service Configuration Mode is used to configure the properties required for a mobile station to interface with a Packet Data Interworking Function (PDIF).



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

aaa attribute

Sets the system attributes for AAA messages.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

aaa attribute { 3gpp2-bsid *string* **| 3gpp2-service-option** *integer* **| calling-station-id** *integer* **| 3gpp2-serving-pcf** *ip-address* **}**

no aaa attribute

default aaa attribute 3gpp2-service-option *integer*

no

Removes a previously configured AAA attribute.

default

Returns the specified aaa attribute to the original default system settings.

3gpp2-bsid *string*

Specifies the base-station ID and consists of the SID + NID + CELLID.
string must contain 12 hexadecimal upper-case ASCII characters.

3gpp2-service-option *integer*

Specifies the radius attribute value when sending authentication and accounting messages as an integer from 0 through 32767. Default: 4095

calling-station-id *integer*

Specifies the calling station phone number as a sequence of 1 through 15 digits.

3gpp2-serving-pcf *ip-address*

Use this command to generate attribute values without creating a new ASR 5000 image.

Usage

If the RADIUS protocol is being used, accounting messages can be sent over a AAA interface to the RADIUS server.
3gpp2-serving-pcf attribute value (if configured) is sent in both RADIUS authentication and accounting messages. If the attribute value is not configured (or explicitly "not configured" using the **no** keyword), RADIUS attributes are still included with just type and length. This is because inclusion/exclusion of RADIUS attributes are still controlled through the dictionary, not via the CLI.

Example

The following command identifies the base station ID:

```
aaa attribute 3gpp2-bsid 0ab2389acb3
```

aaa authentication

Sets the aaa authentication for first and second phase authentication when multiple authentication is configured on the system.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

aaa authentication { { first-phase | second-phase } | { context-name *name* **aaa-group** *name* **} }**

no aaa authentication { first-phase | second-phase }

no aaa authentication { first-phase | second-phase }

Removes any existing authentication configuration.

first-phase context-name *name* **aaa-group** *name*

Specifies the context name and the aaa group name configured in the context for the first authentication phase.

Important: First phase authentication is mandatory when multiple authentication is configured on the system.

- **context-name** *name*: Specifies the context where the aaa server group is defined as an alphanumeric string of 1 through 79 characters.
- **aaa-group** *name*: Specifies the name of the aaa-group to be used for authentication as an alphanumeric string of 1 through 79 characters.

second-phase context-name *name* **aaa-group** *name*

Specifies the context name and the aaa group name configured in the context for the second authentication phase.

- **context-name** *name*: Specifies the context where aaa server group is defined as an alphanumeric string of 1 through 79 characters.
- **aaa-group** *name*: Specifies the name of the aaa-group to be used for authentication as an alphanumeric string of 1 through 63 characters.

Usage

Two phase-authentication happens in IKEv2 setup for setting up the IPSec session. The first authentication uses Diameter AAA EAP method and second authentication uses RADIUS AAA authentication. The same AAA context may be used for both authentications. PDIF service allows you to specify only a single AAA group, which could normally be used for the first authentication method.

A given AAA group only supports either Diameter or RADIUS authentication. If the NAI in the first authentication is different from NAI in the second authentication each NAI can point to a different domain profile in the PDIF. Each domain profile may be configured with each AAA group, one for Diameter and the other for RADIUS.

Example

Use the following to configure first-phase authentication for an aaa group named *aaa-10* in the PDIF context:

```
first-phase context-name pdif aaa-group aaa-10
```

bind

Binds the service IP address to a crypto template and configures the number of sessions the PDIF can support.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

```
bind address address { crypto-template string } [ max-sessions number ]

no bind
```

no

Removes a previously configured binding.

address

Specifies the IP address of the service.

crypto-template *string*

Specifies the name of the crypto template to be bound to the service as an alphanumeric string of 0 through 127 characters.

max-sessions *number*

Specifies the maximum number of sessions to be supported by the service as an integer from 0 to 3000000. Default: 3000000

Usage

Binds the IP address used as the connection point for establishing the IKEv2 sessions to the crypto template. It can also define the number of sessions the PDIF can support.

Example

The following command binds a service with the IP address *13.1.1.1* to the crypto template *T1* and sets the maximum number of sessions to *2000000*:

```
bind address 13.1.1.1 crypto-template T1 max-sessions 200000
```

default

Sets or restores the default condition for the selected parameter.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

default { { aaa attribute 3gpp2-service-option } | duplicate-session-detection | hss { failure-handling mac-address-validation-failure | mac-address-validation | update-profile } | ip source-violation { drop-limit | period } | setup-timeout | subscriber *name* **| username mac-address-stripping } }**

---

aaa attribute 3gpp2-service-option

Configures the default value 4095.

---

duplicate-session-detection

Configures the default to be NAI-based.

---

hss { failure-handling mac-address-validation-failure | mac-address-validation | update-profile }

Configures the HSS server defaults:
failure-handling mac-address-validation-failure: By default, the MAC address is validated by IMS-Sh interface.

- **mac-address-validation**: By default, validating the MAC address is disabled.
- **update-profile**: By default, updating the PDIF profile is disabled.

---

ip source-violation (drop-limit | period }

Configures IP source-violation detection defaults.

- **drop-limit**: Default number of ip source violations permitted in detection period before the call is dropped is 10.
- **period**: Default detection period is 120 seconds.

---

setup-timeout

Default call setup time limit is 60 seconds.

---

subscriber *name*

Configures the default subscriber name. *name* is a string of 1-127 characters.

---

username mac-address-stripping

Default is to disable stripping the MAC address from the username.

Usage

Configures the default settings for a given parameter.

Example

Use the following example to configure the default call setup time limit:

```
default setup-timeout
```

duplicate-session-detection

Configures the PDIF to detect duplicate call sessions using old IMSI or NAI addresses and clear old call information.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] duplicate-session-detection { imsi-based | nai-based }
```

no

Stops duplicate session detection.

default

Configures the default setting, which is NAI-based detection.

imsi-based

Configures the PDIF to detect duplicate call sessions based on the IMSI address.

nai-based

Configures the PDIF to detect duplicate call sessions based on the NAI address. This is the default setting.

Usage

If an MS leaves the Wi-Fi coverage area and subsequently comes back online, it may initiate a new session setup procedure. After both the device authentication with HSS and the subscriber authentication with AAA server are completed, PDIF runs the internal mechanism to see whether there was any other session bound with the same IMSI. If an old session is detected, PDIF starts clearing this old session by sending a proxy-MIP Deregistration request to the HA. PDIF resumes new session setup by sending a proxy-MIP registration request. When the old session is aborted, PDIF sends Diameter STR messages and RADIUS Acct STOP messages to corresponding AAA servers.
PDIF allows duplicate session detection based on either the NAI or IMSI addresses. When detecting based on NAI, it is the first-phase (device authentication) NAI that is used.

Example

The following command configures duplicate session detection to use IMSI addressing:

```
duplicate-session-detection imsi
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

hss

Configures the Home Subscriber Server (HSS) parameters.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

```
hss { failure-handling { { mac-address-validation-failure | update-profile } action {
terminate | continue } } | update-profile | mac-address-validation }

[ no | default ] hss { failure-handling | update-profile | mac-address-validation }
```

no

Removes a previously configured HSS profile.

default

Resets the defaults for this command.

failure-handling mac-address-validation-failure

Configures how the HSS is to handle errors.
If HSS returns a list of MAC addresses and if PDIF fails to match the subscriber MAC address against the list, the session is always terminated.

action { continue | terminate }

Configures the action to be performed depending on the failure type.

- **continue**: Ignores a mac-address-validation-failure and continue the session.
- **terminate**: Terminates the session on a mac-address-validation-failure.

mac-address-validation

If mac-address-validation is enabled, the PDIF queries the HSS for a list of MAC addresses associated with the Mobile Directory Number (MDN). Default: Disabled

update-profile

Update the HSS with the subscriber profile. Default: Disabled

Usage

An HSS provides MAC address validation and store part of the subscriber profile. This command enables or disables validation and profile updates, and configures how the system responds to failures: terminate or continue a session.
An ims-sh-service and Diameter interface need to be configured to communicate with the HSS.

Example

The following example enables *mac-address* validation:

```
hss mac-address-validation
```

ims-sh-service

Associates the IMS-Sh-service parameters.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

ims-sh-service name *name*

no ims-sh-service name *name*

no

Removes a previously configured IMS-Sh-service.

name

Names the IMS-Sh-service in the pdif-service context.

Usage

This command is used to name the IMS-Sh-service.

Example

The following command names the IMS-Sh-service ims1:

```
ims-sh-service name imsi1
```

ip source-violation

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires that the source address of the received packets matches the IP address assigned to the subscriber (either statically or dynamically) during the session.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

ip source-violation { **clear-on-valid-packet** | **drop-limit** *num* | **period** *secs* }

no ip source-violation clear-on-valid-packet

clear-on-valid-packet

Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet. Default: disabled

drop-limit *num*

Sets the number of allowed source violations within a detection period before forcing a call disconnect. If *num* is not specified, the value is set to the default.
num is an integer from 1 to 1000000. Default: 10

period *secs*

Sets the length of time (in seconds) for a source violation detection period to last.
If *secs* is not specified, the value is set to the default.
secs is an integer from 1 to1000000. Default: 120

Usage

This function is intended to allow the operator to configure a network to prevent problems such as when a user gets handed back and forth between two PDIFs a number of times during a handoff scenario.
This function operates in the following manner:
When a subscriber packet is received with a source address violation, the system increments the IP source-violation drop-limit counter and starts the timer for the IP-source violation period. Every subsequent packet received with a bad source address during the IP-source violation period causes the drop-limit counter to increment.
For example, if the drop-limit is set to 10, after 10 source violations, the call is dropped. The period timer continues to count throughout this process.

Example

The following command sets the drop limit to *15* and leaves the other values at their defaults:

```
ip source-violation drop-limit 15
```

mobile-ip

Sets the MIP FA context for the specific PDIF service.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

mobile-ip foreign-agent context *string* **[fa-service** *string* **]**

no mobile-ip

no

Removes previously configured parameters.

foreign-agent context *string*

Specifies the context name in which the FA is configured as an alphanumeric string of 1 through 79 characters.

fa-service *string*

Specifies the name of the FA service in the FA context as an alphanumeric string of 1 through 79 characters.

Usage

Shows in which context the FA is located and names the FA service.

Example

This command configures MIP for the FA context named *fa1*:

```
mobile-ip foreign-agent context fa1
```

setup-timeout

Configures the maximum time allowed to set up a session.

Product

PDIF

Privilege

Security-Administrator, Administrator

Syntax

setup-timeout *integer*

default setup-timeout

setup-timeout *integer*

Specifies the session setup timer (in seconds) as an integer from 2 through 300. Default: 60

default setup-timeout

Defaults the session setup timer to 60 seconds.

Usage

PDIF clears both user session and tunnels if a call does not initiate successfully before the timer expires.

Example

The following command sets the setup-timeout to the default 30 seconds:

```
default setup-timeout
```

username

Configures mac-address-stripping on a username coming in from a mobile station session.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

```
username mac-address-stripping

[ default | no ] username mac-address-stripping
```

username mac-address-stripping

Configures mac-address stripping from the Network Access Identifier (NAI).

default

Configures the default parameter which is **disabled**.

no

Returns the configuration to the default condition.

Usage

When enabled, PDIF strips the MAC address from a mobile username NAI before sending to the RADIUS AAA server.

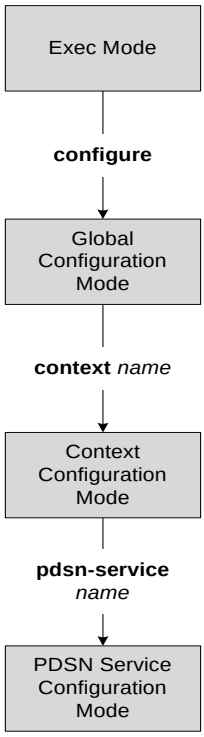
Example

The following example disables mac-address-stripping.

```
no username mac-address-stripping
```

Chapter 229
PDSN Service Configuration Mode Commands

The PDSN Service Configuration Mode is used to create and manage PDSN service instances for the current context.



a11-signalling-packets

Applies DSCP marking for IP header carrying outgoing A11-signalling packets.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

a11-signalling-packetsip-header-dscp *hexa_number*

[**no** | **default**] **a11-signalling-packetsip-header-dscp**

no

Disables the **a11-signalling-packets ip-header-dscp** option configuration.

default

Sets / Restores default value assigned for specified parameter **a11-signalling-packets ip-header-dscp**.

hexa_number

a Hexa decimal number between 0x0 and 0x3F.

Usage

Use this command to configured value of DSCP to be set for all outgoing A11 signaling msg.
By default the CLI is disabled and DSCP is marked as 0 in ip-header.

Example

The following command configures value of DSCP to be set for all outgoing to A11 signaling message *0x3F*:

a11-signalling-packets ip-header-dscp *0x3F*

aaa 3gpp2-service-option

Specifies the value for the 3gpp2-service option.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

aaa 3gpp2-service-option *number*

no aaa 3gpp2-service-option

default aaa 3gpp2-service-option

no

Disables the aaa 3gpp2-service option configuration.

default

Sets / Restores default value assigned for specified parameter **aaa 3gpp2-service-option**.

number

Service option *number* is integer and should be between *0* to *32767*.

Usage

Allows the configuration of a default service option value to be sent in accounting when service option values are not received from PCF. The PDSN will default the service option value to the configured value if the value is not specified by the PCF.

Example

The following command sets the service option to be *40*:

```
aaa 3gpp2-service-option 40
```

aaa nas-ip-address

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

aaa nas-ip-address*IPv4 address*

no aaa nas-ip-address

default aaa 3nas-ip-address

no

Disables the aaa nas-ip-address option configuration.

default

Sets / Restores default value assigned for specified parameter **aaa nas-ip-address** by default this is disabled.

ipv4 address

Specifies the IPv4 addresses to be used.

Usage

Allows the configuration.

Example

The following command configures *1.2.3.4*:

aaa as-ip-addres *1.2.3.4*

access-flow traffic-validation

If **access-flow traffic-validation** is enabled for the service and the subscriber then the flows are checked against the filter rules. If the packets does not match the filter rules, and N violations occur in K seconds, the rp connection is downgraded to best-effort flow, if it is not already a best-effort flow.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

access-flow traffic-validation [**threshold** { **interval** *seconds* | **violations***limit* }]

no access-flow traffic-validation

default access-flow traffic-validation [**threshold** { **interval** | **violations** }]

no

Disable traffic validation for the service.

default

Traffic validation configuration for the service is set to the default value.

threshold { [violations *limit* **] [interval** *seconds* **] }**

violations *limit*: Sets the parameters that determine traffic access violations. This is determined by setting the maximum number of violations within a set time period. must be an integer from *1* through *100000*.
interval *seconds* Sets the time interval, in seconds. must be an integer from *1* through *100000*.

Usage

Use this command to enable traffic validation for the current PDSN service.

Example

The following command enables traffic validation for the current PDSN service and sets the limit allowed to *100* **violations** within *5* seconds:

```
access-flow traffic-validation threshold violations 100 interval 5
```

access-network

Configures access network parameters.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

access-network { **accounting identifier** *identifier_name* | **realm** *realm_name* }

no access-network { **accounting identifier** | **realm** } }

no

Disables the **access-network**.

accounting identifier

Configures accounting for the access-network. This value must be a string from 1 to 128 characters in length.

realm *realm_name*

Configures the realm for the access-network. *realm_name* must be a string from 1 to 128 characters in length.

Usage

Use this command to configure access-network parameters for accounting and realms.

Example

The following command creates an **access-network realm** named *realm2*.

access-networkrealm *realm2*

airlink bad-sequence-number

Configures PDSN behavior for airlink related parameters.

Product

PDSN

Privilege

Security Administrator, Administrator

```
airlink bad-sequence-number { accept | deny [use-deny-code { poorly-formed-request |
unsupported-vendor-id}]}

[ no | default ] airlinkbad-sequence-number
```

no

Disables the deny of bad-sequence number and accept it.

---

default

It is the default behavior.

---

accept

Accepts the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.
It is the default behavior.

---

deny

Rejects the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.
It uses **poorly-formed-request** option by default to deny a request.

---

use-deny-code { poorly-formed-request | unsupported-vendor-id }

These are optional keywords that used with **deny** sub-command to deny the A11 RRQ messages that have either an unsupported vendor Id or A11 Requests with bad/poor formation.
unsupported-vendor-id denies request on the basis of vendor Id.
poorly-formed-request will deny the A11 request on the basis of request formation or structure. It is the default deny code for **deny** sub-command.

Usage

This command is used to configure the airlink parameters for A11 RRQs.
When configured it denies the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.

Example

The following command would configure the system to deny all A11 RRQ messages having unsupported vendor Id or bad structure of message, including those having arilink sequence number less than or equal to a previously received sequence number:

```
airlinkbad-sequence-number deny
```

allow alt-ppp

Allows proprietary modified versions of PPP type sessions to connect this PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
allowalt-ppp

no allow alt-ppp

default allow alt-ppp
```

no

Disables the allowed alternate PPP feature.

default

Sets the specified parameter to default.

Usage

This command is used to deviate from standard PPP protocol and use a proprietary modified version of PPP with a pre-defined non-negotiable PPP parameters.
It is a vendor-specific licensed feature command.

Example

```
allow alt-ppp
```

always-on-indication

Enables/disables the inclusion of 3GPP2 Always On Indicators in messages to the PCF.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
always-on-indication

no always-on-indication
```

no

Disables the sending of 3GPP2 Always On Indication messages.

Usage

This command is available when the 3GPP2 Always-On RP Extensions feature-use license is installed. When enabled, this command causes the PDSN service to include the Always On Indicators in the Normal Vendor Specific Extension (NVSE) part of an A11 Session Update message to the PCF. The indicator will only be sent for those subscriber sessions in which Always On functionality is enabled as determined after a successful authentication: the 3GPP2-Always-On attribute is set to a value of *1* (Active) for subscribers configured on a AAA server, or the always-on parameter is set for locally configured subscribers.
This functionality is enabled by default.

Example

use the following command to Enables the inclusion of 3GPP2 Always On Indicators in messages to the PCF.

```
always-on-indication
```

associate

Associates a PDSN-service with a Quality of Service (QoS) policy.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

associate qci-qos-mapping *string*

no associate qci-qos-mapping

no

Disables the configuration to associate PDSN-serivce with qos policy.

qci-qos-mapping *string*

qci-qos-mapping configures QCI to QoS mapping for this PDSN service.

string a string of size 1 to 63.

Usage

The following is used for configuration to associate PDSN-serivce with qos policy.

Example

associate qci-qos-mapping *sample*

authentication

Configures authentication parameters for specific PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

authentication { [**allow-noauth**] [**chap** *chap_priority*] [**mschap** *mschap_priority*] [**pap** *pap_priority*] } | [**msid-auth**]

default authentication

---

default

Configures authentication parameters for specific PDSN service.

---

allow-noauth

Default: Disabled
This option configures the system to provide subscribers with network access even though they have not been authenticated. This command issued by itself would cause the system to not attempt to authenticate subscribers.
When the allow-noauth option is used in conjunction with commands specifying other authentication protocols and priorities to use, then if attempts to use those protocols fail, the system will treat the allow-noauth option as the lowest priority.
If no authentication is allowed, then NAI construct will be implemented in order to provide accounting records for the subscriber.

---

chap *chap_priority*

Default: 1
This option configures the system to attempt to use the Challenge Handshake Authentication Protocol (CHAP) to authenticate the subscriber.
A *chap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.
chap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference.
CHAP is enabled by default as the highest preference.

---

mschap *mschap_priority*

Default: Disabled
This option configures the system to attempt to use the Microsoft Challenge Handshake Authentication Protocol (MSCHAP) to authenticate the subscriber.
A *mschap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.
mschap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference.

---

pap *pap_priority*

Default: 2

This option configures the system to attempt to use the Password Authentication Protocol (PAP) to authenticate the subscriber.
A *pap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.
pap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference.
PAP is enabled by default as the second highest preference.

msid-auth

Default: Disabled
This option configures the system to attempt to authenticate the subscriber based on their Mobile Station Identity (MSID).

Usage

Use to specify how the PDSN service should handle authentication and what protocols to use. The flexibility is given to configure this option to accommodate the fact that not every mobile will implement the same authentication protocols.
The chassis is shipped from the factory with the authentication options set as follows:

- allow-noauth disabled
- chap enabled with a priority of 1
- mschap disabled
- msid-auth disabled
- pap enabled with a priority of 2

Important: At least one of the keywords must be used to complete the command.

Example

The following command would configure the system to allow no authentication for subscribers and would perform accounting using the default NAI-construct of *username@domain*:

```
authentication allow-noauth
```

The following command would configure the system to attempt subscriber authentication first using CHAP, then MSCHAP, and finally PAP. If the allow-noauth command was also issued, if all attempts to authenticate the subscriber using these protocols fail, then the subscriber would be allowed access:

```
authentication chap 1 mschap 2 pap 3
```

bcmcs

Sets the BCMCS (Broadcast Multicast Service) group username and password for RADIUS access.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

bcmcs { **customptt** | **encrypted grppasswd** *group_passwd* | **flow-id** *value* [**flow-id-type** { **flow-id** | **program-id** }] | **grppasswd** *group_password* | **grpusrname***group_name* | **ptt** { **destination-context** *dest_name* | **disconnect-dscp-label** *dscp_label* | **mtu** *transmission_unit* | **rohc-profile-name** *rohc_profile_name* } }

default bcmcs [**custom ptt** | **ptt** { **disconnect-dscp-label** | **mtu** | **rohc-profile-name** }]

no bcmcs { **custom ptt** | **flow-id value** [**flow-id-type** { **flow-id** | **program-id** } | **grppasswd** | **grpusrname** | **ptt** { **destination-context** | **disconnect-dscp-label** | **mtu** | **rohc-profile-name** } }

custom

Customise the BCMCS configuration.

flow-id *value*

Set the BCMCS flow-id. This value must be a hex string between *0x1000* and *0xFFFFFFFF*.
Making this entry opens a new mode: bcmcs-flow-id.
rohc-profile name : Configure ROHC parameters name, name should be string of size *1* to *63*.

grpusrname *group_name*

Sets the BCMCS group name for RADIUS access requests. This value must be a string from *1* to *127* characters in length.

encrypted grppasswd *group_passwd*

Set the BCMCS group password for RADIUS access requests. This value must be a string from *1* to *63* characters in length.
Password can be encrypted or clear.

ptt {destination-context *dest_name* **| disconnect-dscp-label** *dscp_label***| mtu** *transmission_unit* **| rohc-profile-name** *rohc_profile_name* **}**

destination-context: Specify the intended destination context name. This value must be string of *1* to *79* characters in length.
disconnect-dscp-label: Configures the DSCP label to be present in the In Call Signalling packet based on which In Call Signalling and Media Flows will be disconnected. This value must be a Hexadecimal number between *0x0* and *0xFF*.
mtu *transmission_unit*: Configures maximum transmission unit, This value must be ranging from *100* to *2000*. Default is *1500*.

rohc_profile_name *rohc_profile_name*: Profile name of the ROHC compressor and decompressor. This value should be a string of *1* to *63*.

Usage

Use this command to set the BCMCS group username and password for RADIUS access requests.

Example

bcmcsgrpusername *group_name***bcmcsgrppasswd** *group_password*

bind

Binds the PDSN service to a logical IP interface serving as the R-P interface. Specifies the maximum number of subscribers that can access this service over the interface.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

bindaddress*address* [**max-subscribers** *count*]

no bind address

no

Removes a previously configured binding.

address

Specifies the IP address (address) of the interface configured as the R-P interface. *address* is specified in dotted decimal notation.

max-subscribers *count*

Default: *500000*
Specifies the maximum number of subscribers that can access this service on this interface.
count can be configured to any integer value between *0* and *2500000*.

Important: The maximum number of subscribers supported is dependant on the license key and the number of active PACs/PSCs installed in the system. A fully loaded system with *13* active PACs/PSCs can support *2500000* total subscribers. Refer to the license key command for additional information.

Usage

Associate or tie the PDSN service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an R-P interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.
This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.
When configuring the **max-subscribers** option, be sure to consider the following:

- The total number of interfaces that you will configure for use as R-P interfaces
- The maximum number of subscriber sessions that all of the interfaces may handle during peak busy hours
- The average bandwidth for each of the sessions
- The type of physical port (10/100Base-Tx or 1000Base-T) to which these interfaces will be bound

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

Example

The following command would bind the logical IP interface with the address of *192.168.3.1* to the PDSN service and specifies that a maximum of *600* simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```
bind address 192.168.3.1 max-subscribers 600
```

The following command disables a binding that was previously configured:

```
nobind address
```

data-available-indicator

Enables sending Data Available Indicator extension in R-P Registration Reply.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

[no | default] data-available-indicator

no

Default: Disabled
Disable the sending of the Data Available Indicator extension in R-P Registration Reply.

default

Sets / Restores default value assigned for specified parameter for **data-available-indicator**.

Usage

Use this command to enable or disable the sending of the Data Available Indicator extension in R-P Registration Reply

Example

Use the following command to enable sending the Data Available Indicator extension in R-P Registration Reply:

```
data-available-indicator
```

Use the following command to disable sending the Data Available Indicator extension in R-P Registration Reply

```
no data-available-indicator
```

data-over-signaling

Enables the data-over-signaling marking feature for A10 packets.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] data-over signaling
```

default

Sets / Restores default value assigned for specified parameter for **data-over signaling**

no

Default: Enabled
Disable the data-over signaling feature for A10 packets.

Usage

Use this command to enable or disable the data-over signaling feature for A10 packets.

Important: This is a customer-specific command.

Example

```
no data-over-signaling
```

default subscriber

Specifies the name of a subscriber profile configured within the same context as the PDSN service from which to base the handling of all other subscriber sessions handled by the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

defaultsubscriber *profile_name*

no default subscriber

no

Enables/Disables the option **default subscriber** *profile_name*

profile_name

Specifies the name of the configured subscriber profile. *profile_name* can be between *1* and *127* alpha and/or number characters and is case sensitive.

Usage

Each subscriber profile specifies "rules" such as permissions, PPP settings, and timeout values.
By default, the PDSN service will use the information configured for the subscriber named default within the same context. This command allows for multiple PDSN services within the same context to apply different "rules" to sessions they process. Each set of rules can be configured under a different subscriber name which is pointed to by this command.
Use the **no default subscriber** *profile_name* command to delete the configured default subscriber.

Example

To configure the PDSN service to apply the rules configured for a subscriber named *user1* to every other subscriber session it processes, enter the following command:

default subscriber *user1*

direct-lte-indicator

Enables sending Direct LTE Indicator VSA in Access Request.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] direct-lte-indicator
```

default

Sets / Restores default value assigned for specified parameter for **data-over signaling**

no

Default: Enabled
Disables sending Direct LTE Indicator VSA in Access Request.

Usage

Use this command to enable or disable sending Direct LTE Indicator VSA in Access Request.

Important: This is a customer-specific command.

Example

```
nodirect-lte-indicator
```

dormant-transition

Configures the PDSN behavior to terminate A10 session, when the PDSN receives the A11-RRQ (Type 4) before the session for the original MN is established completely.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] dormant-transition initial-session-setup
```

no

Terminates the A10 session, when PDSN receives the A11-RRQ (Type 4) before the original session established completely.

default

Keeps the A10 session live in case of A11-RRQ (Type 4) is received before the original session is established completely.

Usage

When the status of A10 session goes to dormant before the session for the original MN is established completely, the different MN may possibly send the A11-RRQ (Type 4) to the PDSN and PPP renegotiation may start.
This command is used to terminate the A10 session when the PDSN receives the A11-RRQ (Type 4) before the session for original MN is established completely.

Example

Following command is used to release the A10 session in case of receiving A11-RRQ (Type 4) before the original session is established completely

```
no dormant-transition  initial-session-setup
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

fragment

Enables or disables PPP payload fragmentation.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] fragment ppp-data
```

no

Disables the fragmentation of ppp data.

default

Default enables ppp data fragmentation.

Usage

This command is to indicate to the RP module to NOT fragment PPP payloads being sent to the PCF, if the total packet size (PPP+GRE+IP) exceeds *1500* bytes.
Disabling fragmentation may cause the **sessmgr** to perform outer IP fragmentation of the outgoing packet, if the resulting packet exceeds the MED MTU.

Example

The following command enables PPP payload fragmentation.

```
fragment ppp-data
```

gre

Configures Generic Routing Encapsulation (GRE) parameters for the A10 protocol within the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

gre { **checksum** | **checksum-verify** | **ip-header-dscp** *value* { **all-control-packets** | **setup-packets-only** } | **protocol-type** {**any** | **byte-stream** | **ppp** } | **reorder-timeout** *value* | **segmentation** |**sequence-mode** { **none** | **reorder** } | **sequence-numbers** | **threegppp2-ext-header qos-marking** }

no gre { **checksum** | **checksum-verify** | **ip-header-dscp** | **segmentation** | **sequence-numbers** | **threegppp2-ext-headers qos-marking** }

default gre { **checksum** | **checksum-verify** | **ip-header-dscp** | **protocol-type** | **reorder-timeout** | **segmentation** | **sequence-mode** | **sequence-numbers** | **threegppp2-ext-headers qos-marking** }

---

no

Disables the specified functionality.

---

default

Restores the specified parameter to its default setting.

---

checksum

Default: disabled
Enables the introduction of the checksum field in outgoing GRE packets.

---

checksum-verify

Default: disabled
Enables verification of the GRE checksum (if present) in incoming GRE packets.

---

ip-header-dscp *value* **{ all-control-packets | setup-packets-only }**

Default: Disabled
Used to configure the QoS Differentiated Services Code Point (DSCP) marking for GRE packets.

- *value* : Represents the DSCP setting. It represents the first six most-significant bits of the ToS field. It can be configured to any hex value from 0x0 through 0x3F.
- **all-control-packets** : Dictates that the DSCP marking is to be provided in all GRE control packets.
- **setup-packets-only** : Dictates that the DSCP marking is to be provided only in GRE setup packets.

protocol-type { any | byte-stream | ppp }

Specifies the protocol used fro GRE encapsulation that is acceptable to
any: Specifies that the PDSN service will accept GRE packets encapsulated using any protocol.
byte-stream: Specifies that the PDSN service will accept GRE packets only encapsulated using byte stream. Using byte stream encapsulation, PPP packets are framed at different intervals and sent.
ppp: Specifies that the PDSN service will accept GRE packets only encapsulated using the Point-to-Point Protocol (PPP). Using PPP encapsulation, PPP packets are framed at regular intervals and sent.

reorder-timeout

Default: *100*
Configures max number of milliseconds to wait before processing reordered out-of-sequence GRE packets. *milliseconds* must be an integer from *0* through *5000*.

segmentation

Default: disabled
Enables GRE Segmentation for the PDSN service.

sequence-mode { none | reorder }

Default: none
Configures handling of incoming out-of-sequence GRE packets.
none: Specifies that sequence numbers in packets are ignored and all arriving packets are processed in the order they arrive.
reorder: Specifies that out of sequence packets are stored in a sequencing queue until one of the conditions is met:

- The reorder timeout occurs: All queued packets are sent for processing and the accepted sequence number is updated to the highest number in the queue.
- The queue is full (five packets): All packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number in the queue.
- An arriving packet has a sequence number such that the difference between this and the packet at the head of the queue is greater than five. All the packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number that arrived.
- A packet arrives that fills a gap in the sequenced numbers stored in the queue and creates a subset of packets whose sequence numbers are continuous with the current accepted sequence number. This subset of packets in the queue is sent for processing. The reorder timer continues to run and the accepted sequence number is updated to the highest number in the subset delivered.

sequence-numbers

Enables insertion of GRE sequence numbers in data that is about to be transmitted over the A10 interface. Data coming into the system containing sequence numbers but that is out of sequence is not re-sequenced.

threegppp2-ext-headers qos-marking

When threegppp2-ext-headers qos-marking is enabled and the PCF negotiates capability in the A11 RRQ, the PDSN will include the qos optional data attribute in the GRE 3gpp2 extension header.
The **no** keyword, enables qos-marking in the gre header based on the tos value in the header.

Usage

The **gre protocol-type** command can be used to prevent the PDSN service from servicing PCFs that use a specific form of encapsulation.

Use the **no gre sequence-numbers** command to disable the inclusion of GRE sequence numbers in the A10 data path.

The chassis is shipped from the factory with the authentication options set as follows:

- **protocol-type any**
- sequence-numbers enabled

Example

Use this command to configure the PDSN service to exclude byte stream encapsulated GRE traffic:

gre protocol-type *ppp*

inter-pdsn-handoff mobility-event-indicator

Configures the PDSN to support the Mobility Event Identifier (MEI) during inter-PDSN handoffs. The presence of the Mobility Event Indicator (MEI) and Access Network Identifier (ANID) elements in a A11 handoff request represents an Inter-PDSN handoff.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

inter-pdsn-handoff mobility-event-indicator

no inter-pdsn-handoff mobility-event-indicator

default inter-pdsn-handoff mobility-event-indicator

no

Disables support for the MEI during inter-PDSN handoffs.

default

Sets / Restores default value assigned for **inter-pdsn-handoff mobility-event-indicator**. By default it is disabled.

Usage

Use this command to configure support for the MEI during inter-PDSN handoffs.

Example

Use the following command to enable support for the MEI during inter-PDSN handoffs

```
inter-pdsn-handoff  mobility-event-indicator
```

inter-pdsn-handover

Configures Inter-PDSN handoff related parameters.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

inter-pdsn-handover use-canid-panid

no inter-pdsn-handover use-canid-panid

default inter-pdsn-handover use-canid-panid

no

Disables support for the MEI during inter-PDSN handoffs parameters.

default

Sets / Restores default value assigned for **inter-pdsn-handoff mobility-event-indicator**. By default it is disabled.

Usage

Use this command to configure Inter-PDSN handoff related parameters.

Example

Use the following command to econfigure Inter-PDSN handoff related parameters.

```
inter-pdsn-handover use-canid-panid
```

ip header-compression rohc

Enters PDSN Service ROHC Configuration Mode and allows you to configure ROHC parameters that the PDSN conveys to the PCF in the initial A11 RRP message before PPP authentication.

By default, ROHC is disabled for a PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
ipheader-compression rohc

default ipheader-compression rohc

no ipheader-compression rohc
```

default

Sets all PDSN Service ROHC Configuration Mode values back to the defaults and disable ROHC for this PDSN service.

no

Disable IP header compression for this PDSN Service.

Usage

Use this command to enter the PDSN Service ROHC Configuration Mode or disable ROHC for the current PDSN service.

Example

The following command disables ROHC for the current PDSN service and sets all of the values for commands in PDSN Service ROHC Configuration Mode back to their default settings:

```
no ip header-compression rohc
```

ip local-port

Configures the local User Datagram Protocol (UDP) port for the R-P interfaces' IP socket.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
ip local-port number

default ip local-port
```

number

Default: *699*
Specifies the UDP port number.
number can be any integer value between *1* and *65535*.

default

Designates UDP port, default value as *699*.

Usage

Specify the UDP port that should be used for communications between the Packet Control Function (PCF) and the PDSN.

Important: The UDP port setting on the PCF must match the local-port setting for the PDSN service on the system in order for the two devices to communicate.

Example

Use the following command to specify a UDP port of *3950* for the PDSN service to use to communicate with the PCF on the R-P interface:

```
iplocal-port 3950
```

ip source-violation

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

Product

PDSN, PDIF

Privilege

Security Administrator, Administrator

Syntax

ip source-violation { **clear-on-valid-packet** | **drop-limit** *num* | **period** *secs* | **reneg-limit** *num* }

no ip source-violation clear-on-valid-packet

defaultip source-violation { **drop-limit** | **period** | **reneg-limit** }

no

Enables/Disables **ip source-violation clear-on-valid-packet**.

default

Configure default settings related to **ip source-violation**.

clear-on-valid-packet

Default: disabled
Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

drop-limit *num*

Default: *10*
Sets the number of allowed source violations within a detection period before forcing a call disconnect. If *num* is not specified, the value is set to the default.
num can be any integer value from *1* to *1000000*.

period *secs*

Default: *120*
The length of time, in seconds, for a source violation detection period to last. drop-limit and reneg-limit counters are decremented each time this value is reached.
The counters are decremented in this manner: reneg-limit counter is reduced by one (1) each time the period value is reached until the counter is zero (0); drop-limit counter is halved each time the period value is reached until the counter is zero (0). If *secs* is not specified, the value is set to the default.
secs can be any integer value from *1* to *1000000*.

reneg-limit *num*

Default: *5*
Sets the number of allowed source violations within a detection period before forcing a PPP renegotiation. If *num* is not specified, the value is set to the default.
num can be any integer value from *1* to *1000000*.

Usage

This function is intended to allow the operator to configure a network to prevent problems such as when a user gets handed back and forth between two PDIFs PDSNs a number of times during a handoff scenario.
This function operates in the following manner:
When a subscriber packet is received with a source address violation, the system increments both the IP source-violation reneg-limit and drop-limit counters and starts the timer for the IP-source violation period. Every subsequent packet received with a bad source address during the IP-source violation period causes the reneg-limit and drop-limit counters to increment.
For example, if reneg-limit is set to 5, then the system allows 5 packets with a bad source address (source violations), but on the 5th packet, it re-negotiates PPP.
If the drop-limit is set to *10*, the above process of receiving *5* source violations and renegotiating PPP occurs only once. After the second *5* source violations, the call is dropped. The period timer continues to count throughout this process.
If the configured source-violation period is exceeded at any time before the call is dropped, the reneg-limit counter is checked. If the reneg-limit counter is greater than zero (0), the reneg-limit is decremented by *1*. If the reneg-limit counter equals zero, the drop-limit is decremented by half.

Example

The following command sets the drop limit to *15* and leaves the other values at their defaults:

```
ip source-violation drop-limit 15
```

lifetime

Specifies the time that an A10 connection can exist before its registration is considered expired.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

lifetime *time*

no lifetime

default lifetime

no lifetime

Specifies that an A10 connection can exist for an infinite amount of time.

default lifetime

Sets / Restores default value assigned for **lifetime** as 1800.

time

Default: 1800
Specifies the time that an A10 connection can exist before its registration is considered expired.
time is measured in seconds and can be configured to any integer value between *1* and *65534*.

Usage

Set a limit to the amount of time that a subscriber session can remain up whether or not the session is active or dormant. If the lifetime timer expires before the subscriber terminates the session, their connection will be terminated automatically.
Use the **no lifetime** command to delete a previously configured lifetime setting. If after deleting the lifetime setting you desire to return the lifetime parameter to its default setting, use the **default lifetime** command.

Example

The following command specifies a time of *3600* seconds (1 hour) for subscriber sessions on this PDSN service:

```
lifetime 3600
```

max-retransmissions

Configures the maximum number of times the PDSN service will attempt to communicate with a PCF before it marks it as unreachable.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

max-retransmissions *count*

default max-retransmissions

default

Sets / Restores default value assigned for **max-retransmissions** as *5*.

count

Specifies the maximum number of times the PDSN service will attempt to communicate with a PCF before it marks it as unreachable.
count can be configured to any integer value between *1* and *1,000,000*.

Usage

If the value configured for the max-retransmissions is reached the call will be dropped.
The chassis is shipped from the factory with the Internet maximum number of retransmissions set to *5*.

Example

The following command configures the maximum number of retransmissions for the PDSN service to *3*:

```
max-retransmissions 3
```

mobile-ip foreign-agent context

For Mobile IP support, specifies the context in which the FA service(s) are configured.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
mobile-ip foreign-agent context context_name [  fa-service name  ]
no mobile-ip foreign-agent context
```

no

Enables/Disables **mobile-ip foreign-agent context**

context_name

Specifies the name of the previously configured context that facilitates the FA service(s). context_name must be between *1* and *79* alpha or numeric characters and is case sensitive.

[fa-service *name* **]**

This optional keyword allows you to link the PDSN service to a particular FA service in the specified context. *name* is the name of the FA service to link to. *name* is a string of size *1* to *63*

Usage

FA services on the system can be configured either in the same or different contexts from those facilitating PDSN services. When they are configured in separate contexts, this command configured with a PDSN service instructs the PDSN service to route traffic to the context facilitating the FA service.
Use the **no mobile-ip foreign-agent context** to delete a previously configured destination context.

Example

The following command instructs the PDSN service to use the context named FA-destination for FA functionality:

```
mobile-ip foreign-agent context fa-destination
```

mobile-ipv6

Configures Mobile IPv6 parameters within specific PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

mobile-ipv6 mobile-access-gateway context *context_name* [**mag-service** *name*]

mobile-access-gateway

Configures Mobile Access Gateway (MAG) parameters within specific PDSN service.

context *context_name*

Designates name of the context in which the MAG service is configured. Must be followed by context name of MAG service.

context_name is a string of size 1 to 79.

mag-service *name*

Designates name of the MAG service in that context. Must be followed by MAG service name.

name is a string of size 1 to 63.

Usage

This command is used to configure Mobile IPv6 parameters and Mobile Access Gateway (MAG) parameters within specific PDSN service.

Example

The following command configures Mobile IPv6 parameters and Mobile Access Gateway (MAG) parameters within specific PDSN service.

mobile-ipv6 mobile-access-gateway context *pdsn1* **mag-service** *serv1*

msid length

Configures checking the length of the A11 MSID in A11 Session Specific Extn and airlink records.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
msid length { [ min min_length ] | max max_length }

default msid length
```

default

Specifies the default length of MSID (*10* to *15*) as per standard. By default **msid** is disabled.

min *min_length*

Specifies the minimum length for MSID.
min_length is any Integer value between *10* to *15*, but should be less than *max_length* specified with **max**. Default is *10*.

max *max_length*

Specifies the maximum length for MSID.
max_length is any Integer value between *10* to *15*, but should be more than *min_length* specified with **min**. Default is *15*.

Usage

MSID length can be configured either in the standard length or different customized length form. This command is used to specify the allowed length of MSID.

Example

The following command specifies an MSID length between *12* and *15*:

```
msid length min 12 max 15
```

nai-construction

Specifies a domain alias that will be used to represent the context which the PDSN service should use for AAA functionality.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

nai-construction domain *alias*

no nai-construction domain

domain *alias*

alias represents the "domain" name that you would like to associate with the context in which AAA functionality is configured. alias can be between *1* and *79* alpha and/or numeric characters and is case-sensitive.

Usage

Enabling NAI will be constructed for the subscriber in the event that their mobile station (MS) does not negotiate CHAP, PAP, or MSCHAP. If this option is selected, no further attempts will be made to authenticate the user. Instead, the constructed NAI will be used for accounting purposes.
The context specified by this command would be used to provide the communication with the RADIUS accounting server.
Use the **no nai-constructed** domain command to deleted a configured alias.

Important: This command should only be used if the PDSN service is configured to allow no authentication using the authentication allow-noauth command.

Additionally, the **aaa constructed-nai** command in the Context Configuration mode can be used to configure a password for constructed NAIs.

Example

The following command configured a domain alias of aaa_context for the PDSN service to use when an NAI is constructed for a subscriber session:

```
nai-construction domain aaa_context
```

new-call conflict

Enable or disable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] new-call conflict terminate-session-old-pcf
```

no

Disable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

default

Enable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

Usage

This configuration supports to enable or disable to send A11-RUPD to current PCF, when the system receives the A11-RRQ(Type1) from new PCF during the session exists.
If the configuration is **no new-call conflict terminate-session-old-pcf** system will not send registration update to old PCF on receiving a new call (A11-RRQ(Type1)) request for an existing active/dormant session.
The default behavior is to send registration updates.

Example The following command configured a system to send a registration update on receiving an A11-RRQ (Type 1) request for an existing active/dormant session:

```
new-call conflict terminate-session-old-pcf
```

pcf-monitor

Enables the monitoring of all the PCFs that have sessions associated with it. The PDSN stops monitoring a PCF if it is determined to be down. Once a PCF is determined to be down, the PDSN tears down all sessions that correspond to the PCF and generates AAA Accounting Stop messages. All the PCFs that are connected to the PDSN service are monitored.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

pcf-monitor [**interval** *seconds* | **max-inactivity-time** *seconds* | **num-retry** *num* | **timeout** *seconds*]

[**no** | **default**] **pcf-monitor**

pcf-monitor

Entering the command with no keywords enables the PCF monitoring function with all parameters set to the defaults.

no

Disables the pcf monitoring function.

default

Sets / Restores default value assigned for **pcf-monitor**.

interval *seconds*

Default: 60 seconds
Sets the amount of time to wait between ping request messages.
seconds must be an integer in the range from 1 through 3600.

max-inactivity-time *seconds*

Default: 120 seconds
The maximum amount of time (seconds) with no A10 traffic from a PCF before the ICMP-ping mechanism is triggered.
seconds must be an integer from 1 through 3600.

num-retry *num*

Default: 5
Sets the number of times that the PDSN retries to ping the PCF. When num-retry for a given PCF has been exhausted with no response, sessions that correspond to the non-responsive PCF are terminated and Accounting Stop records for each terminated session are generated.
num must be an integer in the range from 0 through 100.

timeout *seconds*

Default: 3 seconds
The amount of time to wait for a response before retrying.
seconds must be in the range from 1 through 10.

Usage

Use this command to enable the PDSN service to monitor the PCFs that have sessions associated with the PDSN service.

Example

The following command enables PCF monitoring with parameters set to the defaults:

```
pcf-monitor
```

The following command enables PCF monitoring and sets the timeout to *10* seconds:

```
pcf-monitor timeout 10
```

The following command disables pcf-monitoring:

```
no pcf-monitor
```

pcf-session-id-change restart-ppp

Manages current session and PPP renegotiation on GRE-key change without any change in PCF/PANID/CANID. This command disables or enables the PPP renegotiation restart on receiving an RP registration request from the current PCF with GRE key (PCF session Id) change. With this command the PDSN aborts and restarts the call causing PPP renegotiation.

This is enabled by default.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] pcf-session-id-change restart-ppp
```

no

Disables the pcf-session-id-change restart-ppp function.
With this option PDSN does not restart the PPP renegotiation on GRE key change from current PCF in an RP registration request, unless it indicates change in PCF/PANID/CANID.

default

Set the pcf-session-id-change function to the default state on enabled.

Usage

GRE key (PCF session ID) is sued to identify the data packet for a session and is negotiated through the A11 signaling messages between PCF and PDSN. By default PDSN aborts and restart the PPP renegotiation on receipt of any RP registration request with change in GRE key or PCF session Id.
With use of no pcf-session-id-change restart-ppp command PDSN is configured to disable the restart of call or PPP renegotiation on receipt of any RP registration request with changed GRE key, unless it has any PCF/ANID/CANID change. PDSN silently switches the GRE key for the session, retaining the existing PPP session.

Example

The following command disables the PPP renegotiation restart action on receipt of any RP RRQ with changed GRE key from same PCF/PANID/CANID.

```
no pcf-session-id-change  restart-ppp
```

pdsn type0-tft attempt-inner-match

Configures a type0 traffic flow template (tft) to a type1 traffic flow template.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

[no | default] pdsn type0-tft attempt-inner-match

no

Disables **pdsn type0-tft attempt-inner-match**.

default

Sets / Restores default value assigned for **pdsn type0-tft attempt-inner-match.**

Usage

This CLI is used make PDSN match inner IP packets for an AIMS call. When enabled, the PDSN tries to match a type-0 tft to match both outer and inner packet, so that MN can use a Type-0 filter for HoA traffic which are tunneled.
This is disabled by default.

Example

The following command enables type0 tft:

pdsn type0-tft attempt-inner-match

peer-pcf

Configures settings for any PCF that has a connection with this PDSN.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

peer-pcf { *ip_address* | *ip_address/mask* } **bcmcs-framing** { **hdlc-like** | **segment-based** }

ip_address **|** *ip_address/mask*

ip_address must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6.
ip_address/mask must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6, followed by the mask.

bcmcs_framing { hdlc-like | segment-based }

Specifies the type of bcmcs_framing to use for this PCF connection.

- hdlc-like: applies HDLC-like framing for all BCMCS flows
- segment-based: applies segment-based framing for all BCMCS flows

Usage

Use this command to configure the settings for any PCF that is connected to this PDSN. You can also specify bcmcs framing settings to use for the connection.

Example

The following command configures the peer-pcf for an IP address of *131.2.3.4*:

```
peer-pcf 131.2.3.4
```

pma-capability-indicator

Enables sending PMIP Capability Indicator VSA in Access Request.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
pma-capability-indicator  [ 3gpp2 ]

[ no | default ] pma-capability-indicator
```

3gpp2

Use 3GPP2 defined VSA. Default is to use Custom1 VSA.

no

Enables/Disables sending PMIP Capability Indicator VSA in Access Request.

default

Sets / Restores default value assigned for PMIP Capability Indicator.

Usage

Use this command to enable sending PMIP Capability Indicator VSA in Access Request.

Example

The following command enables sending PMIP Capability Indicator using 3GPP2 defined VSA in Access Request.

```
pma-capability-indicator 3gpp2
```

policy

Configures PDSN service policies.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

policy msid-match *msid_with_wildcards* **redirect** *address* [**weight** *weight_num*] [*address2* [**weight** *weight_num*]... *address16* [**weight** *weight_num*]] [**weight** *weight_num*]

no policy msid-match *msid_with_wildcards*

policy overload { **redirect** *address* [**weight** *weight_num*] [*address2* [**weight** *weight_num*] ... *address16* [**weight** *weight_num*]] | **reject** [**use-reject-code** { **admin-prohibited** | **insufficient-resources** }] }

no policy overload [**redirect** *address* [*address2* ... *address16*]]

default policy overload

policy pcf-zone-match *zone_number* **redirect** *address* [**weight** *weight_num*] [*address2* [**weight***weight_num*] ... *address16* [**weight** *weight_num*]]

no policy pcf-zone-match*zone_number*

[**default** | **no**] **policy rrq mei-from-current-pcf suppress-ppp-restart**

policy service-option enforce

[**default** | **no**] **policy service-option**

policy unknown-cvse enforce

[**default** | **no**] **policy unknown-cvse**

no

Enables/Disables the PDSN service policies.

default

Sets / Restores default value assigned for specified PDSN service policies.

policy msid-match *msid_with_wildcards* **redirect** *address* **[weight** *weight_num* **][** *address2* **[weight** *weight_num* **]...** *address16* **[weight** *weight_num* **]][weight** *weight_num* **]**

Specifies how a PDSN service should handle an incoming call that matches a list of wildcard MSIDs.

msid_with_wildcards: An MSID in which up to 16 digits have been replaced with the wildcard '$'. This defines the list of possible matches for incoming calls.

redirect: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.

address: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight *weight_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. *weight_num* must be an integer from 1 through 10.

policy overload { redirect *address* **[weight** *weight_num* **] [** *address2* **[weight** *weight_num* **] ... address16 [weight** *weight_num* **]] | reject [use-reject-code { admin-prohibited | insufficient-resources }] }**

Specifies how a PDSN service should handle an overload condition.

redirect: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.

address: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight *weight_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. *weight_num* must be an integer from 1 through 10.

reject: This option will cause any overload traffic to be rejected. The PDSN will send an A11 Registration Reply Code of 82H (insufficient resources).

use-reject-codeadmin-prohibited: When this keyword is specified and traffic is rejected, the error code admin prohibited is returned instead of the error code insufficient resources. This is the default behavior.

use-reject-codeinsufficient-resources: When this keyword is specified and traffic is rejected, the error code insufficient resources is returned instead of the error code admin prohibited.

policy pcf-zone-match *zone_number* **redirect** *address* **[weight** *weight_num* **] [** *address2* **[weight***weight_num* **]** *... address16* **[weight** *weight_num* **]]**

Specifies how a PDSN service should handle an incoming call that matches a predefined zone number.

zone_number: An integer between 1 and 32 that defines the zone incoming calls must match for redirection.

redirect: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.

address: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight *weight_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. *weight_num* must be an integer from 1 through 10.

policy rrq mei-from-current-pcf suppress-ppp-restart

rrq configures policy for PPP restart after getting mei in rrq.

mei-from-current-pcf mei is received in rrq from current pcf.

suppress-ppp-restart suppresses ppp restart when mei is received in rrq from current pcf

policy service-option enforce

service-option configures R-P service-option to use for specific PDSN service. Must be followed by valid service-option number, ranging from 0 to 1000.

enforce designates enforcement of R-P service-option number.

policy unknown-cvse enforce

unknown-cvse configures PDSN service unknown cvse policy.

enforce enforces unknown cvse policy where unknown CVSEs in RRQs will cause Deny

Usage

Policies can be implemented to dictate PDSN service behavior for various conditions such as overloading. The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system.
The system automatically invokes the overload policy when an on-line software upgrade is started.
Use the **no policy** { **overload** | **service-option** } command to delete a previously configured policy. If after deleting the policy setting you desire to return the policy parameter to its default setting, use the **default policy** command.
The chassis is shipped from the factory with the policy options set as follows:

- overload disabled
- sequence-numbers enforced enabled

Caution: Incorrect configuration of the **policy msid-match** and **policy pcf-zone-match** keywords could result in sessions failing to be established. For example, if PDSN1 is configured to redirect sessions to PDSN2 while PDSN2 is configured to redirect sessions to PDSN1, a loop is created in which all sessions would fail to be connected. In addition, sessions will not be established if the PDSN to which the sessions are being redirected is unavailable.

Example

The following command configures the PDSN service to redirect traffic to two different destinations with weights of *1* and *10* respectively:

```
policy overload redirect 192.168.1.100 weight 1 192.168.1.200 weight 10
```

ppp

Sets PPP tunneling parameters for subscribers in the current PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
ppp { tunnel-context context_name | tunnel-type { l2tp | none } }

 [ no | default ] ppp tunnel-type
```

no

Enables/Disables the PPP tunneling parameters for subscribers in the current PDSN service.

default

Sets / Restores default value assigned for PPP tunneling parameters for subscribers in the current PDSN service.

tunnel-context *context_name*

The name of the context that has a LAC service configured to handle all tunnels from this PDSN service.

tunnel-type { l2tp |none }

l2tp: Force all subscriber sessions in this PDSN service to use L2TP tunneling.
none: Do not force L2TP tunneling. This is the default.

Important: If the context specified by the **ppp tunnel-context** *context_name* command does not have a LAC service configured and **tunnel-type** is set to **l2tp** or the call is rejected.

Important: If the PPP tunnel context has not been set or has been cleared with the **no ppp tunnel-context** command and **tunnel-type** is set to **l2tp**, the context where the current PDSN service resides is used. If that context does not have a LAC service configured the call is rejected.

Usage

Use this command to enable or disable forced L2TP tunneling for all subscribers using this PDSN service. Also use this command to define which context defines the L2TP tunneling parameters.

Example

To set the tunnel context to the context named *context1* and enable forced L2TP tunneling, use the following commands;

```
ppp tunnel-context context1ppp tunnel-type l2tp
```

To enable forced L2TP tunneling with IPSEC security, use the following commands;

```
ppp tunnel-type l2tp-secure
```

To disable forced tunneling, use the following command;

```
ppp tunnel-type none
```

To clear the setting for the tunnel context, use the following command;

```
no ppp tunnel-context
```

qos-profile-id-mapping

Creates the customized QoS profile identifier to QoS mapping for IMS authorization support.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

```
qos-profile-id-mapping profile-idid_num { [ description desc ] | [ downlink-bw dl_bw] | [
drop-rate drop_percentage ] | [ latency latency_duration ] | [ qos-class { class-A |
class-B | class-C | class-D | class-E | calss-F } ] | [ uplink-bwul_bw ] } +

[ default | no ] qos-profile-id-mappingprofile-id id_num
```

default

Configures the specified QoS profile ID for QoS mapping with default values in this PDSN service.

no

Removes the configured QoS profile ID mapping in this PDSN service.

profile-id *id_num*

Specifies the profile identifier for QoS parameters to be used as the customized profile ID or modifies the QoS parameters in a profile ID (*id_num*) coming from RAN.
id_num must be an integer between 0 and 65535.

description *desc*

Specifies the user defined description for profile identifier.
desc must be an alpha and/or numeric string between 1 and 32 characters.

downlink-bw *dl_bw*

Default: 32
Specifies the downlink (towards the MN) data traffic bandwidth in kilo-bits per second for this QoS profile.
dl_bw must be an integer value between 0 and 100000.

drop-rate *drop_percentage*

Default: 0
Specifies the permitted packet drop rate in percentage for traffic flow to this QoS profile.
drop_percentage must be an integer value between 0 and 1000.

latency *latency_duration*

Default: 1000
Specifies the permitted latency duration in milli-seconds for this QoS profile.
latency_duration must be an integer value between 0 and 1000.

qos-class {class-A | class-B | class-C | class-D | class-E | class-F }

Default: Class-C
Specifies the type of QoS class associated with this QoS profile
class-A: Specifies the A type of QoS class.
class-B: Specifies the B type of QoS class.
class-C: Specifies the C type of QoS class.
class-D: Specifies the D type of QoS class.
class-E: Specifies the E type of QoS class.
class-F: Specifies the F type of QoS class.

uplink-bw *ul_bw*

Default: 32
Specifies the uplink (from the MN) data traffic bandwidth in kilo-bits per second for this QoS profile.
ul_bw must be an integer value between 0 and 100000.

+

More than one of the above keywords can be entered within a single command.

Usage

Use this command to define the values associated with the profile ID on the PDSN. This profile ID is used during the mapping to and from the authorized QoS to the QoS parameters for the A10 link. This mapping is required because the PDSN only knows the profile IDs and not the actual configured values for the profile ID in the RAN. Also this configuration allows the use of custom profile IDs for the subscribers.
If no values are defined with a QoS profile ID, the values from matching QoS profile ID from RAN will be applicable to the subscriber traffic.

Example

The following command sets the downlink bandwidth to *32* kbps, latency duration as *1000* ms, uplink bandwidth to *32* kbps, and QoS class to Class-C for the QoS profile ID *11* in a PDSN service:

```
default qos-profile-id-mapping profile-id 11
```

qos update

Sets QoS update parameters for policy mismatches or wait timeouts.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
qos-update { policy-mismatch | wait-timeout seconds action { disconnect-session |
downgrade-to-best-effort | drop-packets } }

 [ no | default ] qos-update { policy-mismatch | wait-timeout }
```

no

Enables/Disables the **qos-update** [**policy-mismatch** | **wait-timeout**].

default

Sets / Restores default value for **qos-update** [**policy-mismatch** | **wait-timeout**].

policy-mismatch

PDSN raises a TFT violation if there is a QoS policy mismatch.

wait-timeout *seconds* **action { disconnect-session | downgrade-to-best-effort | drop-packets }**

Sets the wait time for A11 RRQ for QoS changes. *seconds* must be an integer from 1 through 1000.
action: configures the action on the wait-timeout

- **disconnect-session**: Drops the call if the A11 RRQ has not been received for the QoS update. This includes all of the IP flows for the session.
- **downgrade-to-best-effort**: Drops packets if the A11 RRQ has not been received for the QoS update. Sends the forward traffic over best effort (flow FF or FE if available).
- **drop-packets**: Drops packets if the A11 RRQ has not been received for the QoS update.

Usage

This command provides a PDSN service level configurable to configure an action, if the PCF ignores the QoS Update request from PDSN. It sets the amount of time to wait and the action to take, if no RRQ is received before the timeout. The action can be to drop packets for the flow, disconnect the session or to downgrade to best effort.

Example

```
qos-update policy-mismatch
```

The following command sets **wait-timeout** to *60* seconds and invokes **downgrade-to-best-effort** if the A11 RRQ has not been received for the QoS update:

```
qos-update wait-timeout 60 actiondowngrade-to-best-effort
```

registration-accept

Allows the PDSN to accept registration requests when a handoff disconnect is in progress. When the PDSN is tearing down a session and the MN moves over to a new PCF and initiates a new session, the PDSN by default does not accept the handoff until it tears down the old session.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ]registration-accept handoff session-disconnect-in-progress
```

no

Disable accepting of registration requests when a handoff disconnect is still in progress.

default

Default is disabled.
Sets / Restores default value assigned for **registration-accept handoff session-disconnect-in-progress**.

Usage

Use this command to allow the PDSN service to accept registration requests when a handoff disconnect is still in progress.

Example

```
registration-accept handoffsession-disconnect-in-progress
```

registration-ack-deny terminate-session-on-error

Configures the PDSN service to terminate an A11 session when a Registration ACK received from the PCF has an error status.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ]registration-ack-deny terminate-session-on-error
```

no

Disable terminating A11 sessions on a Registration ACK error from the PCF.

default

Sets / Restores default value assigned to **registration-ack-deny terminate-session-on-error**.

Usage

Use this command to enable the PDSN service to terminate A11 sessions on a Registration ACK error from the PCF.

Example

Use the following command to enable this functionality in the PDSN:

```
registration-ack-deny terminate-session-on-error
```

registration-deny

Configures parameters related to registration rejection.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

registration-deny { **handoff** { **closedrp-rp handoff-in-progress** | **connection-setup-record-absent** [**use-deny-code** { **poorly-formed-request** | **reason-unspecified** } | **max-deny-reply-limit** *num* | **mismatched-coa-source-address** | **new-call** { **connection-setup-record-absent** | **reverse-tunnel-unavailable** } | **session-already-active** | **session-already-closed** | **session-already-dormant** | **terminate-session-on-error** | **use-zero-gre-key**}

[**default** |**no**] **registration-deny** { **handoff** { **closedrp-rp handoff-in-progress** | **connection-setup-record-absent** } | **mismatched-coa-source-address** | **new-call** { **connection-setup-record-absent** | **reverse-tunnel-unavailable** } | **session-already-active** | **session-already-closed** | **session-already-dormant** | **terminate-session-on-error** | **use-zero-gre-key**}

default

Sets / Restores default value for **registration-deny**.

no

Disables the specified option.

handoff { closedrp-rp handoff-in-progress | connection-setup-record-absent [use-deny-code { poorly-formed-request | reason-unspecified }

This command configures the handoff behavior.
closedrp-rp handoff-in-progress: Configures parameters related to denying handoffs from Closed-RP to RP systems. When enabled the PDSN rejects retransmitted handoff R-P requests when a handoff is already in progress from Closed RP to RP. The deny code used is 'Reason Unspecified'. The default is disabled meaning that the PDSN simply discards such requests.
connection-setup-record-absent [**use-deny-code** { **poorly-formed-request** | **reason-unspecified** }]: When enabled the PDSN denies or discards handoff R-P sessions that do not have an Airlink Connection Setup record in the A11 Registration Request. Default is disabled. Default PDSN behavior is to accept such requests.
[**use-deny-code** { **poorly-formed-request** | **reason-unspecified** }: Sets the specified Registration Deny Code when denying a handoff because of a missing connection setup record.

max-deny-reply-limit *num*

Default: 3
Configures max number of retries of erroneous registration request message from PCF for a session before PDSN terminates the session. *num* can be from 1 to 10.

mismatched-coa-source-address

Default: disabled

Denies RP requests which have a care-of-address field that is different from the request source address.

---

new-call { connection-setup-record-absent [use-deny-code { poorly-formed-request | reason-unspecified } | reverse-tunnel-unavailable }

connection-setup-record-absent: Configures the PDSN to reject calls that do not have the airlink connection setup record in the RRQ.
use-deny-code { **poorly-formed-request** | **reason-unspecified** } When rejecting calls that do not have the airlink setup record, use the specified deny code.
reverse-tunnel-unavailable: Configures the PDSN to reject calls if the GRE key for a user collides with that of another user.

---

session-already-active

PDSN denies Registration requests for sessions that are already active with the error code “poorly formed request” .

---

session-already-closed

PDSN denies RP renew and dereg requests with error code 0x8E for absent R-P sessions.

---

session-already-dormant

PDSN denies Registration requests for sessions that are already dormant with the error code “poorly formed request” .

---

terminate-session-on-error

Default: Disabled.
Configures PDSN to terminate session if erroneous registration request message is received for the session.

---

use-zero-gre-key

Configures the PDSN to set the GRE key to zero (0) when denying a new R-P session.

Usage

Use this command to configure parameters relating to the rejection of registration requests.

Example

To reject calls that do not have the airlink setup record in the RRQ, enter the following command:

```
registration-deny new-call connection-setup-record-absent
```

To reject calls if the GRE key collides with that of another user, enter the following command:

```
registration-deny new-call reverse-tunnel-unavailable
```

To set the GRE key to 0 (zero) when a new R-P session is denied, enter the following command:

```
registration-deny new-call use-zero-gre-key
```

registration-discard

Configures the PDSN service to discard any Registration Request message containing multiple information elements of the same type or a different GRE key for existing IMSI session.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] registration-discard { bad-extension | gre-key-change |
handoffconnection-setup-record-absent }
```

default

Sets / Restores default value assigned for **registration-discard** .

no

Disables the discarding of Registration request messages containing multiple information elements or different GRE keys.

bad-extension

Default: Disabled
Configures the PDSN to discard Registration Request message containing multiple information elements of same type.

gre-key-change

Default: Disabled
Configures PDSN to discard Registration Request message containing different GRE key for existing IMSI session. Default is disable

handoff connection-setup-record-absent

Default: Disabled
When enabled, discards A11 Handoff requests that do not contain the Airlink Setup record.

Usage

Use this command to configure the PDSN service to discard and Registration Requests that contain multiple information elements of the same type or discard Registration Requests that contain GRE keys that have different GRE keys for the existing IMSI session.

Example

To configure the PDSN service to discard of Registration Requests that have multiple information elements of the same type, enter the following command:

```
registration-discard bad-extension
```

To configure the PDSN service to discard registration Requests that contain a GRE key that is different than the existing one for the existing IMSI session, enter the following command:

```
registration-discard gre-key-change
```

registration-update

Configures registration update related parameters for the PDSN.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

registration-update { **pdsn-code-nvse** | **wait-timeout** *secs* **}**

[**default** | **no**] **registration-update** { **pdsn-code-nvse** | **wait-timeout }**

no

If this option is used with the **pdsn-code-nvse** keyword, then pdsn-code-nvse configuration is disabled.
If this option is used with the **wait-timeout** keyword, a separate A11 timer is not used. The PDSN waits for the ppp retransmit-timeout and then sends the A11 Update. If a value is provided, then the "ppp retransmit-timeout" is ignored and a separate A11 timeout is started immediately upon sending the LCP Term-Ack. The A11 Update is then sent when the timer expires.
A value of 0 sends the A11 Update immediately after sending the LCP Term-Ack.

default

Sets / Restores default value assigned for **registration-update** { **pdsn-code-nvse** | **wait-timeout }**

pdsn-code-nvse

Adds the PDSN code NVSE in all A11 registration update messages.

secs

The number of seconds to wait. *secs* must be an integer in the range from 0 through 16.

wait-timeout

After the Mobile Node terminates a PPP session between the PDSN and the Mobile Node, the PDSN service waits for the specified time period to receive an A11 RRQ from the PCF before it sends out a Registration-Update to clear the Session from the PCF.

Usage

Use this command to configure registration update related
The **wait-tiimeout** keyword configures the PDSN to wait the specified amount of time before sending out a Registration-Update to clear the Session from the PCF.

Example

Use the following command to set the registration wait-timeout to *16* seconds:

```
registration-update wait-timeout 16
```

retransmission-timeout

Configures the maximum allowable time for the PDSN service to wait for a response from the PCF before it a) attempts to communicate with the PCF again (if the system is configured to retry the PCF) or b) marks the PCF as unreachable.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

retransmission-timeout *time*

[**default** | **no**] **retransmission-timeout**

no

Enables/Disables the **retransmission-timeout**.

default

Sets / Restores default value assigned for **retransmission-timeout**.

time

Specifies the maximum allowable time for the PDSN service to wait for a response from the PCF before it a) attempts to communicate with the PCF again (if the system is configured to retry the PCF) or b) marks the PCF as unreachable.
time is measured in seconds and can be configured to any integer value between 1 and 1,000,000.

Usage

Use the retransmission timeout command in conjunction with the **max-retransmissions** command in order to configure the PDSN services behavior when it does not receive a response from a particular PCF.
Use the **no retransmission-timeout** command to delete a previously configured timeout value. If after deleting the lifetime setting you desire to return the lifetime parameter to its default setting, use the **default retransmission-timeout** command.
The chassis is shipped from the factory with the retransmission timeout set to 3 seconds.

Example

The following command configures a retransmission timeout value of *5* seconds:

```
retransmission-timeout 5
```

The following command deletes a previously configured retransmission-timeout setting:

```
noretransmission-timeout
```

service-option

If the service option policy is enabled, this command specifies the service options supported by the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

service-option *number*

no service-option *number*

no

Enables/Disables the **service-option** *number*

default

Sets / Restores default value assigned for **service-option**.

number

Default: 7, 15, 22, 23, 24, 25, 33, 59, 67
Specifies a specific Service Option (SO) number that this PDSN service is allowed to support.
number can be configured to any integer value between 1 and 1000.

Usage

Use the service option command in conjunction with the policy service option enforce command to configure specific SO numbers that are supported. If a particular SO number is not configured, then any subscriber session received with that SO number will be rejected and an A11 Registration Reply Code of 86 (poorly formed request) will be sent.
By default, PDSN services are configured to support the following service option numbers:

- 7: PCF specific
- 15: PCF specific
- 22: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS1 forward, RS1 reverse)
- 23: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS1 forward, RS2 reverse)
- 24: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS2 forward, RS1 reverse)
- 25: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS2 forward, RS2 reverse)
- 33: 3G High Speed Packet Data
- 59: High Rate Packet Data
- 67: RP A10 connection

Important: Option 67 is used for auxiliary connections for Rev-A calls. PPP encapsulation of data packets does not flow over this service option connection. ROHC can be performed without PPP for this service option.

Use the **no service-option** *number* command to delete a previously configured service option. If after deleting the service option setting you desire to return the service option parameter to its default setting, use the **default service-option command**.

Example

The following command enables a service option of *12*:

```
service-option 12
```

The following command disables the default service option *59* :

```
no service-option 59
```

setup-timeout

Specifies the maximum amount of time allowed for session setup.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

[no]setup-timeout *seconds*

default setup-timeout

default

Sets / Restores default value assigned for **setup-timeout**.

seconds

Default: 60 seconds
The maximum amount of time, in seconds, to allow for setup of a session. *seconds* must be an integer from 1 through 1000000

Usage

Use this command to set the maximum amount of time allowed for setting up a session.

Example

Use the following command to set the maximum time allowed for setting up a session to *300* seconds:

setup-timeout *300*

simple-ip allow

Enables or disables Simple-IP sessions from making a connection before authorization takes place.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[no | default ] simple-ip allow
```

no

When a session attempts PPP authentication, it is assumed that it is a Simple-IP session and it is disconnected before the user is authenticated (RADIUS or local authentication). Also, if **allow-noauth** is enabled and PPP authentication is not performed, after IPCP the session is disconnected if it is discovered that it is a Simple-IP session.

default

Reset this command to allow Simple-IP sessions to connect.

Usage

Use this command to prevent Simple-IP sessions from connecting to a PDSN service.

Example

The following command configures the PDSN service so that it will reject any Simple-IP sessions:

```
nosimple-ip allow
```

The following command configures the PDSN service to allow Simple-IP sessions:

```
simple-ip allow
```

spi

Configures the security parameter index (SPI) between the PDSN service and the PCF. This command also configures the redirection of call based on PCF zone.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
spiremote-address { pcf_ip_address | ip_addr_mask_combo } spi-number number {
encrypted secret enc_secret | secret secret } [ description string ] [ hash-
algorithm { md5 | rfc2002-md5 } ] [ replay-protection { nonce | timestamp } ] [
timestamp-tolerance tolerance ] [ zone zone_id ]

no spi remote-address pcf_ip_address spi-number number
```

remote-address { *pcf_ip_address* | *ip_addr_mask_combo* }

pcf_ip_address: Specifies the IP address of the PCF. pcf_ip_address is an IP address expressed in IP v4 dotted decimal notation.
ip_addr_mask_combo: Specifies the IP address of the PCF and specifies the IP address network mask bits. *ip_addr_mask_combo* must be specified using the form 'IP Address/Mask Bits' where the IP address must either be an IPv4 address expressed in dotted decimal notation or an IPv6 address expressed in colon notation and the mask bits are a numeric value which is the number of bits in the subnet mask.

spi-number *number*

Specifies the SPI (number) which indicates a security context between the PCF and the PDSN in accordance with IOS 4.1 and RFC 2002.
number can be configured to any integer value between 256 and 4294967295.

encrypted secret *enc_secret* **| secret** *secret*

Configures the shared-secret between the PDSN service and the PCF. The secret can be either encrypted or non-encrypted.
encrypted secret *enc_secret*: Specifies the encrypted shared key (enc_secret) between the PCF and the PDSN service. enc_secret must be between 1 and 254 alpha and/or numeric characters and is case sensitive.
secret *secret*: Specifies the shared key (secret) between the PCF and the PDSN services. secret must be between 1 and 127 alpha and/or numeric characters and is case sensitive.
The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

description *string*

This is a description for the SPI. *string* must be an alpha and or numeric string of from 1 through 31 characters.

hash-algorithm { md5 | rfc2002-md5 }

Default: md5
Specifies the hash-algorithm used between the PDSN service and the PCF.
md5: Configures the hash-algorithm to implement MD5 per RFC 1321.
rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

replay-protection { nonce | timestamp }

Default: timestamp
Specifies the replay-protection scheme that should be implemented by the PDSN service.
nonce: Configures replay protection to be implemented using NONCE per RFC 2002.
timestamp: Configures replay protection to be implemented using timestamps per RFC 2002.

timestamp-tolerance *tolerance*

Default: 60
Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. If this is set to 0, then time stamp tolerance checking is disabled at the receiving end.
tolerance is measured in seconds and can be configured to any integer value between 0 and 65535.

zone *zone_id*

Specifies the different PCF zones to configure in PDSN service. Mapping of a zone-number to a set of PDSNs can be done per PDSN service basis.
zone_id must be an integer value between 1 and 32. A maximum of 32 PCF zones can be configured for a PDSN service.

Usage

An SPI is a security mechanism configured and shared by the PCF and the PDSN service. Please refer to IOS 4.1 and RFC 2002 for additional information.
Multiple SPIs can be configured if the PDSN service is communicating with multiple PCFs.

Important: The SPI configuration on the PCF must match the SPI configuration for the PDSN service on the system in order for the two devices to communicate properly.

Use the **no** version of this command to delete a previously configured SPI.
This command used with **zone** *zone_id* redirects all calls on the basis of PCF zone to the specific PDSN on the basis of parameters configured at policy pcf-zone-match command.

Example

The following command configures the PDSN service to use an SPI of 256 when communicating with a PCF with the IP address 192.168.0.2. The key that would be shared between the PCF and the PDSN service is q397F65.

```
spi remote-address 192.168.0.2 spi-number 256 secret q397F65
```

The following command deletes the configured SPI of *400* for an PCF with an IP address of *172.100.3.200*:

```
no spi remote-address 172.100.3.200 spi-number 400
```

The following command creates the configured SPI of *400* for an PCF with an IP address of *172.100.3.200* and zone id as 11:

spi remote-address *172.100.3.200* **spi-number** *400* **zone** *11*

tft-validation wait-timeout

Configures the TFT validation wait timeout value for QoS changes. The QoS update timer triggers automatic QoS updates based on dynamic policies.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

tft-validation wait-timeout *seconds*

[**default** | **no**] **tft-validation wait-timeout**

no

Removes the wait-timeout timer.

default

Sets / Restores default value assigned for **tft-validation wait-timeout**.

Usage

Configures the TFT validation wait time value for A11 RRQ for QoS changes. *seconds* must be an integer from 1 through 65535.

Example

Use the following command to set the TFT validation wait-timeout to *5* seconds:

```
tft-validation wait-timeout 5
```

threshold a11-ppp-send-discard

Sets an alarm or alert for the PDSN service based on the number of packets that the PPP protocol processing layer internally discarded on transmit for any reason.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
threshold a11-ppp-send-discard high_thresh [ clear low_thresh ]

no threshold a11-ppp-send-discard
```

no

Deletes the alert or alarm.

high_thresh

Default: *0*
The high threshold number of discarded PPP send packets that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between *0* and *100000*.

clear *low_thresh*

Default:*0*
The low threshold number of discarded PPP send packets that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between *0* and *100000*.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of discarded PPP send packets is equal to or greater than a specified number.
Alerts or alarms are triggered for the number of discarded PPP send packets is based on the following rules:

- **Enter condition:** Actual number of discarded PPP send packets > High Threshold
- **Clear condition:** Actual number of discarded PPP send packets £ Low Threshold

Example

The following command configures a number of discarded PPP send packets threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold a11-ppp-send-discard 1000 clear 500
```

threshold a11-rac-msg-discard

Sets an alarm or alert based on the number of Discarded A11 Registration Acknowledgements for the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
threshold a11-rac-msg-discard high_thresh [  clear low_thresh ]

no threshold a11-rac-msg-discard
```

no

Deletes the alert or alarm.

high_thresh

Default: 0
The high threshold number of Discarded A11 Registration Acknowledgements that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

clear *low_thresh*

Default: *0*
The low threshold number of Discarded A11 Registration Acknowledgements that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between *0* and *100000*.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of Discarded A11 Registration Acknowledgements is equal to or greater than a specified number.
Alerts or alarms are triggered for the number of Discarded A11 Registration Acknowledgements based on the following rules:

- **Enter condition:** Actual number of Discarded A11 Registration Acknowledgements > High Threshold
- **Clear condition:** Actual number of Discarded A11 Registration Acknowledgements £ Low Threshold

Example

The following command configures a number of Discarded A11 Registration Acknowledgements threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold a11-rac-msg-discard 1000 clear 500
```

threshold a11-rrp-failure

Sets an alarm or alert based on the number of A11 Registration Response failures for the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

threshold a11-rrp-failure *high_thresh* [**clear** *low_thresh*]

no threshold a11-rrp-failure

no

Deletes the alert or alarm.

high_thresh

Default: 0
The high threshold number of A11 Registration Response failures that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

clear *low_thresh*

Default:0
The low threshold number of A11 Registration Response failures that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of A11 Registration Response failures is equal to or greater than a specified number.
Alerts or alarms are triggered for the number of A11 Registration Response failures based on the following rules:

- **Enter condition:** Actual number of A11 Registration Response failures > High Threshold
- **Clear condition:** Actual number of A11 Registration Response failures £ Low Threshold

Example

The following command configures a number of A11 Registration Response failures threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold a11-rrp-failure 1000 clear 500
```

threshold a11-rrq-msg-discard

Sets an alarm or alert based on the number of Discarded A11 Registration Requests for the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

threshold a11-rrq-msg-discard*high_thresh* [**clear** *low_thresh*]

no threshold a11-rrq-msg-discard

no

Deletes the alert or alarm.

high_thresh

Default: 0
The high threshold number of Discarded A11 Registration Requests that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

clear *low_thresh*

Default:0
The low threshold number of Discarded A11 Registration Requests that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of Discarded A11 Registration Requests is equal to or greater than a specified number.
Alerts or alarms are triggered for the number of Discarded A11 Registration Requests based on the following rules:

- **Enter condition:** Actual number of Discarded A11 Registration Requests > High Threshold
- **Clear condition:** Actual number of Discarded A11 Registration Requests £ Low Threshold

Example

The following command configures a number of Discarded A11 Registration Requests threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold a11-rrq-msg-discard 1000 clear 500
```

threshold init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for the context.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

threshold init-rrq-rcvd-rate *high_thresh* [**clear** *low_thresh*]

no threshold init-rrq-rcvd-rate

---

no

Deletes the alert or alarm.

---

high_thresh

Default: 0
The high threshold average number of calls setup per second must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between *0* and *1000000*.

---

clear *low_thresh*

Default:0
The low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between *0* and *1000000*.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the average number of calls setup per second is equal to or greater than a specified number of calls per second.
Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter condition:** Actual number of calls setup per second > High Threshold
- **Clear condition:** Actual number of calls setup per second £ Low Threshold

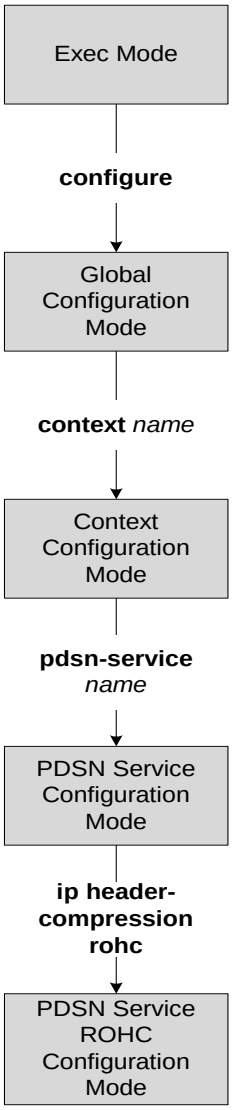
Example

The following command configures a number of calls setup per second threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold init-rrq-rcvd-rate 1000 clear 500
```

Chapter 230
PDSN Service RoHC Configuration Mode Commands

The PDSN Service RoHC Configuration Mode is used to configure RoHC (Robust Header Compression) parameters the PDSN service conveys to the PCF in the initial A11 RRP message before PPP authentication.



Important: The commands, keywords and variables in this mode are available dependent on platform type, product version, and installed license(s).

cid-mode

Enters the RoHC Profile Compression Options Configuration mode.and configures options that apply during RoHC compression for the current RoHC profile.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

cid-mode { large | small } max-cid *integer*

default cid-mode

default

Reset all options in the RoHC Profile Compression Configuration mode to their default values.

large

Use large packets with optional information for RoHC

small

This is the default packet size.
Use small RoHC packets.

max-cid *integer*

Default: 15
The highest context ID number to be used by the compressor. *integer* must be an integer from 0 through 15 when small packet size is selected and must be an integer from 0 through 31 when large packet size is selected.

Usage

Use this command to set the RoHC packet size and define the maximum

Example

The following command sets large RoHC packet size and sets the maximum CID to 100:

```
cid-mode large max-cid 100
```

The following command sets the cid-mode to the default settings of small packets and max-cid 0:

```
default cid-mode
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

mrru

Sets the size of the largest reconstructed reception unit, in octets, that the decompressor is expected to reassemble from segments. The size includes the CRC. If MRRU is negotiated to be 0, no segment headers are allowed on the channel.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

mrru *num_octets*

default mrru

default

reset the value of this command to its default setting

num_octets

Default: 0
This is the number of octets for the maximum size of the largest reconstructed reception unit allowed. *num_octets* must be an integer from 0 through 65535.

Usage

Use this command to set the size, in octets, of the largest reconstructed reception unit, in octets, that the decompressor is expected to reassemble from segments.

Example

The following command sets the largest reconstructed reception unit to 1024 octets:

```
mrru 1024
```

The following command resets the mrru size to its default of 0 octets:

```
default mrru
```

profile

Specifies the header compression profiles to use. A header compression profile is a specification of how to compress the headers of a specific kind of packet stream over a specific kind of link. At least one profile must be specified.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
profile { [ esp-ip ] [ rtp-udp ] [ udp-ip ] [ uncompressed-ip ] }

default profile
```

default

Default: esp-ip rtp-udp udp-ip uncompressed-ip
This command sets the RoHC profile configuration back to its default setting.

esp-ip

This enables RoHC Profile 0x0003 which is for ESP/IP compression, compression of the header chain up to and including the first ESP header, but not subsequent subheaders.

rtp-udp

This enables RoHCProfile 0x0001 which is for RTP/UDP/IP compression

udp-ip

This enables RoHC Profile 0x0002 which is for UDP/IP compression, compression of the first 12 octets of the UDP payload is not attempted.

uncompressed-ip

This enables RoHC Profile 0x0000 which is for sending uncompressed IP packets.

Usage

Us this command to specify the RoHC header compression profiles to use.

Example

The following command sets the profiles to use as esp-ip and rtp-udp:

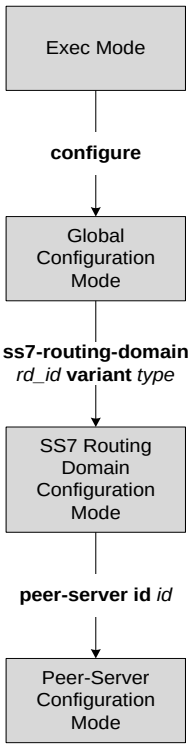
```
profile esp-ip rtp-udp
```

Chapter 231
Peer-Server Configuration Mode Commands

The Peer-Server configuration mode provides the commands to define and manage the peer server configuration part of the SS7 routing on an SGSN.

In this mode, the prompt line usually appears similar to:

```
[local]hostname(config-ss7-rd-<ss7rd_id>-ps-id-<ps_id>)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the configuration mode and returns to the Global configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Return to the Global configuration mode.

mode

Configures the operational mode of the peer-server.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
mode ( loadshare | standby )
```

loadshare

Sets the peer-server to load share. This is the default.

standby

Sets the peer-server to be in standby mode.

Usage

Configure the operational mode of the peer-server.

Example

Configure the peer-server for standby mode.

```
mode standby
```

name

Defines the unique identification - the name - of the peer-server in the SS7 routing domain.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

name *name*

no name

no

Removes the peer server's name from this configuration instance.

name

name: Must be a string of 1 to 64 alphanumeric characters to define a unique identification for the peer-server within the specific SS7 routing domain. Double quotes must be used to create a name that includes spaces.

Usage

Create peer server names that are easy to remember and uniquely identify the PSP.

Example

Use this command to create an easily remembered alphanumeric name for the peer-server:

```
name "Berlin West"
```

psp

Creates the peer-server-process (PSP) instance and enters the PSP configuration mode. See the PSP Configuration Mode chapter in this guide for information on the configuration commands.

Important: This command configures a mandatory parameter in the configuration of the peer server.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] psp instance id
```

no

Removes the PSP instance from the peer server configuration.

id

id Uniquely identifies the specific peer-server-process configuration. The Id must be an integer from 1 to 4.

Usage

Use this command to define the peer-server-process (PSP) instance ID number for the SGSN configuration.

Example

Use this command to create instance #3 for the PSP configuration:

```
psp instance 3
```

routing-context

Defines the ID of the routing context for the peer-server to use.

Important: This command configures a mandatory parameter in the configuration of the peer server.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

routing-context *id*

no routing-context

id

id Uniquely identifies a specific routing context for the peer-server-process to use. The Id must be an integer from 1 to 65535.

no

Removes the routing-context definition from the peer server configuration.

Usage

Use this command to define routing contexts for the peer server.

Example

Define routing-context instance 15:

```
routing-context 15
```

self-point-code

This command defines the point-code to identify the SGSN as a peer server.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

self-point-code *point-code*

no self-point-code

point-code

Point-code is an SS7-type address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC Range.
- a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

no

Removes the self-point-code configuration for this linkset in the peer server.

Important: Removing the self-point-code will result in the termination of all traffic on this link.

Usage

Use this command to define the point-code to identify the SGSN.

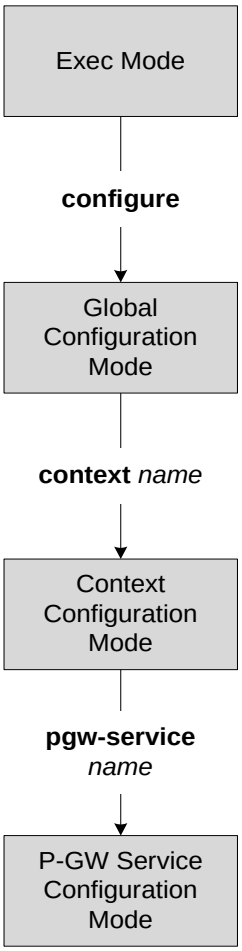
Example

Use the following command to remove the self-point-code definition from the peer-server configuration:

```
no self-point-code
```

Chapter 232
P-GW Service Configuration Mode Commands

The P-GW (PDN Gateway) Service Configuration Mode is used to create and manage the relationship between specified services used for either GTP or PMIP network traffic.



associate

Associates the P-GW service with specific pre-configured services and/or policies configured in the same context.

Product

P-GW

Privilege

Administrator

Syntax

```
associate { egtp-service name [ lma-service name ] | ggsn-service name | lma-service name
[ egtp-service name ] | qci-qos-mapping name }

no associate { egtp-service | lma-service | qci-qos-mapping }
```

no

Removes the selected association from this service.

{ egtp-service *name* **[lma-service** *name* **] | lma-service** *name* **[egtp-service** *name* **] }**

egtp-service *name* **[lma-service** *name* **]**: Specifies that the P-GW service is to be associated with an existing eGTP service within this context.
name must be an alphanumeric string of 1 through 63 characters and be an existing eGTP service.
Configure an associated LMA service name to support handoffs between PMIPv6 and GTP. *name* must be an alphanumeric string of 1 through 63 characters and be an existing LMA service.
lma-service *name* **[egtp-service** *name* **]**: Specifies that the P-GW service is to be associated with an existing LMA service within this context.
name must be an alphanumeric string of 1 through 63 characters and be an existing LMA service.
Configure an associated eGTP service name to support handoffs between PMIPv6 and GTP. *name* must be an alphanumeric string of 1 through 63 characters and be an existing eGTP service.

ggsn-service *name*

Specifies that the P-GW service is to be associated with an existing GGSN service within this context.
name must be an alphanumeric string of 1 through 63 characters and be an existing GGSN service.

qci-qos-mapping *name*

Specifies that the P-GW service is to be associated with an existing QCI-QoS mapping configuration within this context.
name must be an alphanumeric string of 1 through 63 characters and be an existing QCI-QoS mapping configuration.
QCI-Qos mapping is typically configured in a AAA context. Refer to the *QCI-QoS Mapping Configuration Mode Commands* chapter for more information.

Usage

Use this command to associate the P-GW service with other pre-configured services and/or policies configured in the same context.

Example

The following command associates this service with an eGTP service called *egtp1*:

```
associate egtp-service egtp1
```

authorize-with-hss

This command enables or disables subscriber session authorization via a Home Subscriber Server (HSS) over an S6b Diameter interface. This feature is required to support the interworking of GGSN with P-GW and HA.

Product

P-GW

Privilege

Administrator

Syntax

```
authorize-with-hss [ report-ipv6-addr ]

[ default | no ] authorize-with-hss
```

[default | no]

Disables the default authorization of subscriber over S6b interface. Resets the command to the default setting of "authorize locally" from an internal APN authorization configuration.

report-ipv6-addr

Enables the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface.

Usage

Use this command to enable/disable the authorization support for subscriber over S6b interface, which is used between P-GW and the 3GPP AAA to exchange the information related to charging, GGSN discovery, etc.

dns-client

Specifies the DNS client context to use for sending DNS queries.

Product

P-GW

Privilege

Administrator

Syntax

dns-client context *name*

[default | no] dns-client context

default

Returns the command to the default setting of targeting the DNS client in the context where the P-GW service resides.

no

Disables DNS queries.

context *name*

Specifies the name of the context where the DNS client is used for the resolution of PCSCF-FQDN received from S6b interface.
name must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to specify the context where the DNS client resides to perform P-CSCF-FQDN resolution from the S6b interface.

Example

The following command identifies the *egress1* context as the context where the DNS client resides:

```
dns-client context egress1
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

fqdn

Configures a Fully Qualified Domain Name for this P-GW service used in messages between the P-GW and a 3GPP AAA server over the S6b interface.

Product

P-GW

Privilege

Administrator

Syntax

fqdn host *domain_name* **realm** *realm_name*

[default | no] fqdn

default

Returns the command to the default setting of "null".

no

Removes the configured FQDN from this service configuration.

host *domain_name*

Specifies the domain name of the P-GW service.
domain_name must be an alphanumeric string of 1 through 255 characters.

realm *realm_name*

Specifies the realm name of the P-GW service.
realm_name must be an alphanumeric string of 1 through 255 characters.

Usage

Use this command to identify the P-GW service using an FQDN required when sending messages over the S6b interface to a 3GPP AAA server.

Important: In order to properly interact with other nodes in the network, the FQDN should be less than or equal to 96 alphanumeric characters.

Topology Matching (eHRPD only)

You may specify which P-GW you wish an HSGW interface to connect with by enabling topology matching within the FQDNs for both the HSGW service and P-GW service. Topology matching selects geographically closer nodes and reduces backhaul traffic for a specified interface.

The following optional keywords enable or disable topology matching when added to the beginning of an FQDN:

- **topon.***interface_name*.

Beginning an FQDN with **topon** initiates topology matching with available HSGWs in the network. Once this feature is enabled, the rest of the FQDN is processed from right to left until a matching regional designator is found on a corresponding HSGW FQDN.

- **topoff.***interface_name*.

  By default, topology matching is disabled. If you enable topology matching for any interfaces within a node, however, all interfaces not using this feature should be designated with **topoff**.

Example

The following command configures the FQDN for this P-GW service as *123abc.all.com* with a realm name of *all.com*:

```
fqdn host 123abc.all.com realm all.com
```

The following command configures this P-GW service with an FQDN that enables topology matching:

```
fqdn host topon.interface_name.pgw01.bos.ma.node.epc
.mnc<value>.mcc<value>.3gppnetwork.org realm
node.epc.mnc.mcc.3gppnetwork.org
```

Important: The associated HSGW service must have a corresponding FQDN similar to the following:

```
topon.interface_name.hsgw01.bos.ma.node.epc.mncvalue.mccvalue.3gppnetwork
.org
```

gx-li

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

newcall

Configures the P-GW to accept or reject requests for a static IP address if the address is already in use by another session.

Product

P-GW

Privilege

Administrator

Syntax

```
newcall duplicate-subscriber-requested-address { accept | reject }

no newcall duplicate-subscriber-requested-address
```

no

Returns the command to the default setting of "reject".

duplicate-subscriber-requested-address { accept | reject }

Default: **reject**
accept: Specifies that the old session with the requested address will be ended to accept the new session with the same address.
reject: Specifies that the new session requesting the same address will be rejected.

Usage

Use this command to configure the behavior of the P-GW service when receiving requests for static IP address already in use by other sessions.

Important: This command is only applicable to sessions using services supporting duplicate address abort. These services include HA, GGSN, and P-GW.

Example

The following command allows for the acceptance of requests for static IP addresses already in use by other sessions:

```
newcall duplicate-subscriber-requested-address accept
```

plmn

Configures Public Land Mobile Network identifiers used to determine if a mobile station is visiting, roaming, or belongs to this network.

Product

P-GW

Privilege

Administrator

Syntax

plmn id mcc *number* **mnc** *number* **[primary]**

id mcc *number* **mnc** *number*

mcc *number*: Specifies the mobile country code (MCC) portion of the PLMN identifier.
number is the PLMN MCC identifier and must be an integer from 100 through 999.
mnc *number*: Specifies the mobile network code (MNC) portion of the PLMN identifier.
number is the PLMN MNC identifier and can be configured to a 2- or 3-digit integer from 00 through 999.

primary

When multiple PLMN IDs are configured, the **primary** keyword can be used to designate one of the PLMN IDs to be used for the AAA attribute.

Usage

The PLMN identifier is used to aid the P-GW service in the determination of whether or not a mobile station is visiting, roaming, or home. Multiple P-GW services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each P-GW Service.

Example

The following command configures the PLMN identifier with an MCC of *462* and MNC of *02*:

```
plmn id mcc 462 mnc 02
```

session-delete-delay

Configures a delay in terminating a session.

Product

P-GW

Privilege

Administrator

Syntax

session-delete-delay timeout [*msec* **]**

[default | no] session-delete-delay timeout

default

Resets the command to the default setting of 10000 milliseconds.

no

Disables the feature.

timeout *msec*

Default: 10000
Specifies the time to retain the session (in milliseconds) before terminating it.
msec must be an integer from 1000 to 60000.

Usage

Use this command to set a delay to provide session continuity in break-before-make scenarios.

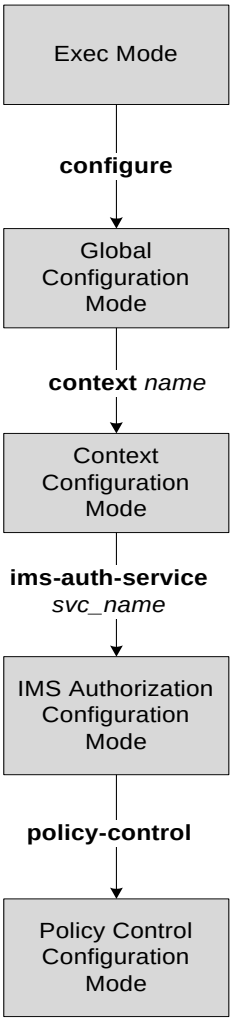
Example

The following command sets the session delete delay to the default setting of 10,000 milliseconds:

```
session-delete-delay timeout
```

Chapter 233
Policy Control Configuration Mode Commands

Policy Control Configuration mode is used to configure the Diameter dictionary, origin host, host table entry and host selection algorithm for IMS Authorization service.



apn-name-to-be-included

This command configures the APN name to be included in CCR Gx messages.

Product

GGSN, IPSG, P-GW

Privilege

Security Administrator, Administrator

Syntax

```
apn-name-to-be-included { gn | virtual }

default apn-name-to-be-included
```

gn | virtual

Specifies which APN name must be sent in the Gx messages.
gn: Specifies to send the real APN name.
virtual: Specifies to send the virtual APN name if present, else to send the real APN name.

default

Applies the default setting for this command.
Default: **gn**

Usage

Use this command to configure the APN name to be included in the CCR Gx messages to the PCRF — the real APN name or the virtual APN name.

Example

The following command configures sending the real APN name in Gx messages:

```
apn-name-to-be-included gn
```

arp-priority-level

This command enables mapping of the ARP priority-level value received from PCRF to inter-user-priority value and be sent in A11 session update.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
arp-priority-level map-to inter-user-priority

[ default | no ] arp-priority-level map-to
```

default

Configures the default setting for this command.
Default: arp-priority-level to inter-user-priority mapping not applicable

no

Disables arp-priority-level to inter-user-priority mapping.

Usage

Important: This command is for a customer-specific implementation to support IP-CAN policy control via Gx interface in PDSN, wherein the PCRF informs the subscriber's subscription level (such as gold, silver, bronze) to PDSN/PCEF via Priority-Level AVP, then PDSN maps the subscriber's subscription level to inter-user-priority and transmits it to PCF via A11 session update message. For more information on the use of this command contact your Cisco account representative.

cc-profile

This command configures the value of the **Offline** AVP sent to the PCRF based on the Charging Characteristics (CC) profile received from the SGSN.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
cc-profile cc_profile_number [ to cc_profile_number_range_end ] map-to offline-avp { 0 |
1 }

{ default | no } cc-profile
```

default

Configures the default setting for this command.
Default: Deletes all previously configured mappings.

no

Deletes all previously configured mappings.

cc_profile_number

Specifies the CC profile number to map.
For example, 1 for Hot Billing.
cc_profile_number must be an integer from 0 through 15.

cc_profile_number_range_end

Specifies, for a range of CC profile numbers to map, the end number. That is, from *cc_profile_number* through *cc_profile_number_range_end*.
cc_profile_number_range_end must be an integer from 1 through 15.

map-to offline-avp { 0 | 1 }

Specifies to map the CC profile number(s) to the **Offline** AVP value sent to the PCRF.

- **0**: Corresponds to the value DISABLE_OFFLINE (0).
- **1**: Corresponds to the value ENABLE_OFFLINE (1).

Usage

Use this command to configure the CC Profile to **Offline** AVP value mapping. The **Offline** AVP's value (DISABLE_OFFLINE (0), ENABLE_OFFLINE (1)) is derived based on the CC profile received from the SGSN as specified by this mapping.
The following example shows how this command can be configured multiple times:

```
cc-profile 1 to 2 map-to offline-avp 1
```

```
cc-profile 4 map-to offline-avp 0

cc-profile 8 map-to offline-avp 1
```

On configuring the above set of commands, the Offline AVP value is sent as 1 (Offline enabled) for the CC profiles 1 (Hot Billing), 2 (Flat Rate), and 8 (Post-Paid). And, as 0 (Offline disabled) for the CC profile 4 (Pre-paid).
When configuring this command, overlapping of CC profile numbers is not permitted. In the following example, after configuring the first command, which specifies to send the **Offline** AVP's value as 1 (Offline enabled) for the CC profiles 1 through 15, the second command, which specifies to map CC profile 7, is not permitted:

```
cc-profile 1 to 15 map-to offline-avp 1

cc-profile 7 map-to offline-avp 0
```

Example

The following command specifies to send **Offline** AVP value as 1 (Offline enabled) for the CC profile 1 (Hot Billing):

```
cc-profile 1 map-to offline-avp 1
```

The following command specifies to delete all previously configured mappings:

```
no cc-profile
```

custom-reauth-trigger

This command enables custom reauthorization event triggers.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
custom-reauth-trigger { none | { preservation-changed | reactivation-changed } + }

default custom-reauth-trigger
```

none

Disables all custom event triggers.
This is the default setting.

preservation-changed

Enables preservation-changed event trigger.

Important: This keyword is for use with a customer-specific implementation, and will be available only if a valid license is installed.

reactivation-changed

Enables reactivation-changed event trigger.

Important: This keyword is for use with a customer-specific implementation, and will be available only if a valid license is installed.

default

Configures the default setting for this command.

Usage

Use this command to enable/disable custom reauth event triggers.
It is recommended that the preservation-changed and reactivation-changed triggers both be enabled. As, when the bearer goes into preservation mode with the preservation-changed trigger, the reactivation-changed trigger must also be enabled for the bearer to get reactivated subsequently.
If only the preservation-changed trigger is enabled, and the bearer goes into preservation mode, the bearer will never get reactivated. The reactivation triggers will be ignored. If only the reactivation-changed trigger is enabled, reactivation of the already active bearer does not take place, and the reactivation triggers are ignored.

Example

The following command disables all custom event triggers:

```
custom-reauth-trigger none
```

diameter dictionary

This command specifies the Diameter Policy Control Application dictionary to be used by the IMS Authorization Service for the policy control application.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter dictionary { Standard | dpca-custom1 | dpca-custom10 | dpca-custom11 | dpca-custom12 | dpca-custom13 | dpca-custom14 | dpca-custom15 | dpca-custom16 | dpca-custom17 | dpca-custom18 | dpca-custom19 | dpca-custom2 | dpca-custom20 | dpca-custom3 | dpca-custom4 | dpca-custom5 | dpca-custom6 | dpca-custom7 | dpca-custom8 | dpca-custom9 | gx-wimax-standard | gxa-3gpp2-standard | gxc-standard | pdsn-ty | r8-gx-standard | std-pdsn-ty | ty-plus | ty-standard }

default diameter dictionary

dpca-custom1

Custom-defined Diameter dictionary for the Gx interface.

dpca-custom2

Custom-defined Diameter dictionary for Rel. 7 Gx interface.

dpca-custom3

Custom-defined Diameter dictionary for the Gx interface in conjunction with IP Services Gateway (IPSG).

dpca-custom4

Standard Diameter dictionary for 3GPP Rel. 7 Gx interface.

dpca-custom5

Custom-defined Diameter dictionary for Rel. 7 Gx interface.

dpca-custom6 ... dpca-custom20

Custom-defined Diameter dictionaries.

gx-wimax-standard

Gx WiMAX standard dictionary.

gxa-3gpp2-standard

Gxa 3GPP2 standard dictionary.

gxc-standard

Gxc standard dictionary.

pdsn-ty

This keyword is restricted.

r8-gx-standard

R8 Gx standard dictionary.

standard

Standard Diameter dictionary for the 3GPP Rel. 6 Gx interface.
Default: Enabled for Gx support in 3GPP networks.

std-pdsn-ty

This keyword is restricted.

ty-plus

This keyword is restricted.

ty-standard

This keyword is restricted.

default

Sets the default Diameter dictionary.
Default: **standard**

Usage

Use this command to specify the Diameter dictionary for IMS Authorization Service.

Example

The following command sets the **standard** dictionary for Diameter Policy Control functions in 3GPP network:

```
diameter dictionary standard
```

diameter host-select reselect

This command controls pacing of the reselection or switching of the PCRF after a change occurs in the table configuration for an IMS Authorization Service.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter host-select reselect subscriber-limit *subs_limit* **time-interval** *duration*

[default | no] diameter host-select reselect

subscriber-limit *subs_limit*

Specifies the limit of subscribers to switch or reselect the PCRF for subscribers not more than *subs_limit* in time duration of *duration* second(s).
subs_limit must be an integer from 1 through 10000000.

time-interval *duration*

Specifies the time duration, in seconds, to reselect PCRF for subscribers not more than *subs_limit* in time duration of *duration* second(s).
duration must be an integer from 1 through 3600.

default

Applies the default setting for this command.
Sets the PCRF reselection or switching to default state.

no

Removes the configured PCRF reselection method and disables the reselection or switching of PCRF.

Usage

Use this command to specify the pacing of reselection or switching of the PCRF in an IMS authorization service..
In case IMS authorization session have been opened on certain PCRF on the basis of the current selection table, and the current active table configuration is changed, the IMSA starts selection procedure for the PCRF. Existing sessions on current PCRF from earlier table is required to close and reopened on the selected PCRF from the new table. This reselection periodicity is controlled by this command and it indicates the number of subscriber sessions *subs_limit* to be reselected or moved in *duration* seconds.
For example, if this command is configured with *100* subscribers and *2* seconds, then the system reselects the PCRF for no more than *100* subscribers per *2* seconds.

Example

The following command sets the system to reselect the new PCRF for no more than *1000* subscriber in *15* seconds:

diameter host-select reselect subscriber-limit *1000* **time-interval** *15*

diameter host-select row-precedence

This command adds/appends rows with precedence to a Diameter host table or MSISDN prefix range table.

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter host-select row-precedence *precedence_value* **table { { { 1 | 2 } host** *host_name* **[realm** *realm_id* **] [secondary host** *host_name* **[realm** *realm_id* **]] } | { prefix-table { 1 | 2 } msisdn-prefix-from** *msisdn_prefix_from* **msisdn-prefix-to** *msisdn_prefix_to* **host** *host_name* **[realm** *realm_id* **] [secondary host** *sec_host_name* **[realm** *sec_realm_id* **] algorithm { active-standby | round-robin }] } } [-noconfirm]**

no diameter host-select row-precedence *precedence_value* **table { { 1 | 2 } | prefix-table { 1 | 2 } }**

---

diameter host-select row-precedence *precedence_value* **table { 1 | 2 } host** *host_name* **[realm** *realm_id* **] [secondary host** *sec_host_name* **[realm** *sec_realm_id* **]]**

This command adds/appends a row in the specified Diameter host table.
In 8.0, a maximum of 16 rows can be added to a table. In 8.1 and later releases, a maximum of 128 rows can be added per table.
row-precedence *precedence_value*: Specifies precedence of the row in the Diameter host table.

Important: In 8.1 and later releases, *precedence_value* must be an integer from 1 through 128. In 8.0 and previous releases, *precedence_value* must be an integer from 1 through 100.

table { 1 | 2 }: Specifies the Diameter host table to add/append the primary and secondary Diameter host addresses.
host *host_name*: Specifies the primary host name. *host_name* must be an alphanumeric string of 1 through 127 characters in length.
realm *realm_id*: Specifies the primary realm ID. *realm_id* must be an alphanumeric string of 1 through 127 characters in length.
secondary host *sec_host_name* **[realm** *sec_realm_id* **]**: Specifies the secondary host name and realm ID:
host *sec_host_name*: Specifies the secondary host name. *host_name* must be an alphanumeric string of 1 through 127 characters in length.
realm *sec_realm_id*: Specifies the secondary realm ID. *realm_name* must be an alphanumeric string of 1 through 127 characters in length.

---

no diameter host-select row-precedence *precedence_value* **table prefix-table { 1 | 2 } }**

Removes the row with the specified precedence from the specified MSISDN prefix range table.

diameter host-select row-precedence *precedence_value* **table prefix-table { 1 | 2 } msisdn-prefix-from** *msisdn_prefix_from* **msisdn-prefix-to** *msisdn_prefix_to* **host** *host_name* **[realm** *realm_id* **] [secondary host** *sec_host_name* **[realm** *sec_realm_id* **] algorithm { active-standby | round-robin }] [-noconfirm]**

Use this command to configure the MSISDN prefix range based PCRF selection mechanism for Rel. 7 Gx interface support, wherein the PCEF is required to discover and select an appropriate PCRF to establish control relationship at primary PDP context activation.
This command adds a row in the specified MSISDN prefix range table. A maximum of 128 rows can be added per prefix range table.
row-precedence *precedence_value*: Specifies precedence of the row in the table.

Important: In 8.1 and later releases, *precedence_value* must be an integer from 1 through 128. In 8.0 and previous releases, *precedence_value* must be an integer from 1 through 100.

prefix-table { 1 | 2 }: Specifies the MSISDN prefix range table to add the primary and/or secondary Diameter host addresses.
msisdn-prefix-from *msisdn_prefix_from*: For a range of MSISDNs, specifies the starting MSISDN.
msisdn-prefix-to *msisdn_prefix_to*: For a range of MSISDNs, specifies the ending MSISDN.

Important: To enable the Gx interface to connect to a specific PCRF for a range of MSISDNs/subscribers configure *msisdn_prefix_from* and *msisdn_prefix_to* with the starting and ending MSISDNs respectively. The MSISDN ranges must not overlap between rows. To enable the Gx interface to connect to a specific PCRF for a specific MSISDN/subscriber, configure both *msisdn_prefix_from* and *msisdn_prefix_to* with the same MSISDN.

host *host_name*: Specifies the primary host name. *host_name* must be an alphanumeric string of 1 through 127 characters in length.
realm *realm_id*: Specifies the primary realm ID. *realm_id* must be an alphanumeric string of 1 through 127 characters in length.
secondary host *sec_host_name* **[realm** *sec_realm_id* **]**: Specifies the secondary host name and realm ID: **host** *sec_host_name*: Specifies the secondary host name. *sec_host_name* must be an alphanumeric string of 1 through 127 characters in length.
realm *sec_realm_id*: Specifies the secondary realm ID. *sec_realm_id* must be an alphanumeric string of 1 through 127 characters in length.
algorithm { active-standby | round-robin }: Specifies the algorithm for selection between primary and secondary servers in the MSISDN prefix range table.
Default: **active-standby**
active-standby: Specifies selection of servers in the Active-Standby fashion.
round-robin: Specifies selection of servers in the Round-Robin fashion.

Important: The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.

-noconfirm

Specifies that the command is to execute without any additional prompt and confirmation from the user.

no diameter host-select row-precedence *precedence_value* **table { 1 | 2 }**

Removes the row with the specified precedence from the specified Diameter host table.

Usage

Use this command to add, update, or delete rows specified with a precedence from a Diameter host table or MSISDN prefix range table.
In the Rel. 7 Gx implementation, when the Gateway interworks with multiple PCRFs, the Gateway can configure the primary and secondary server based on the MSISDN-prefix range in the MSISDN prefix range table. Using this command, you can add a new prefix row into the MSISDN prefix table.
If a row with the precedence that you add already exists in a table, the existing prefix row is removed and the new row is inserted with the same precedence.

Example

The following command adds a row with precedence *12* in table **2** with primary host name as *star_ims1* and secondary host name as *star_ims2* to Diameter host table.

```
diameter host-select row-precedence 12 table 2 host star_ims1 secondary
host star_ims2
```

diameter host-select table

This command selects the Diameter host table or the MSISDN prefix range table, and the algorithm to select rows from the Diameter host table.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
diameter host-select table { { 1 | 2 } algorithm { ip-address-modulus [ prefer-ipv4 |
prefer-ipv6 ] | msisdn-modulus | round-robin } | prefix-table { 1 | 2 } }

[ default | no ] diameter host-select table
```

`diameter host-select table { 1 | 2 } algorithm { ip-address-modulus | msisdn-modulus | round-robin }`

`table { 1 | 2 }`: Specifies the Diameter host table to obtain the primary and secondary host name for PCRF.

`algorithm { ip-address-modulus [ prefer-ipv4 | prefer-ipv6 ] | msisdn-modulus | round-robin }`: Specifies the algorithm to select row from the Diameter host table.

Default: **`round-robin`**

- **`ip-address-modulus [ prefer-ipv4 | prefer-ipv6 ]`**: This algorithm divides the IP address, in binary, of the subscriber by the number of rows in the table, and the remainder is used as an index into the specified table to select the row.
- prefer-ipv4: Specifies that IPv4 addresses are to be used, if an IPv4v6 call is received, for selecting the rows in the host table.
- prefer-ipv6: Specifies that IPv6 addresses are to be used, if an IPv4v6 call is received, for selecting the rows in the host table.
- **`msisdn-modulus`**: This algorithm divides the MSISDN value in binary without the leading "+" of the subscriber by the number of rows in the table, and the remainder is used as an index in the specific table to select the row.
- **`round-robin`**: This algorithm rotates all rows in the active table for selection of the row in round-robin fashion. If no algorithm is specified this is the default behavior.

Important: The Round Robin algorithm is effective only over a large number of selections, and not at a granular level.

`diameter host-select table prefix-table { 1 | 2 }`

Specifies the MSISDN Prefix Range table to be used in case of MSISDN prefix range based PCRF discovery mechanism.

`default`

Applies the default setting for this command.

no

Removes previous configuration.
When no table is selected, the system will not communicate with any PCRF for new sessions.

Usage

Use this command to configure the Diameter host table and row selection methods to select host name or realm for PCRF.
When this command is used to change which table the system should be using, user must re-determine which E-PDF the system should be using for each subscriber. If a different E-PDF results from the configuration change in the table, the system will wait for all of the IMS sessions for the subscriber to be no longer active and then the system either closes/opens Gx sessions with the old/new PDFs respectively, or the system deactivates the PDP contexts of the subscriber.
Here is an example of how row selection is configured for three hosts that the system will use for load-balancing. Operator can configure six rows in a table, as follows.

Modulo 6	Primary Host	Secondary Host
0	1	2
1	1	3
2	2	1
3	2	3
4	3	1
5	3	2

In the above table, the three hosts are named 1, 2, and 3. When all hosts are working, the load will be distributed among all the three hosts. If host 1 fails, then the load will be distributed between the remaining two hosts. In this scenario, the modulo 6 results of 2 and 4 will return rows that have primary hosts but no working back-up host.
In the Rel. 7 Gx implementation, the GGSN/PCEF is required to discover and select an appropriate PCRF to establish control relationship at primary PDP context activation. The ip-address-modulus, msisdn-modulus, and round-robin algorithms are supported by the GGSN/PCEF for PCRF discovery. In addition, the active/standby and round-robin algorithms are used for selection between primary and secondary servers based on the MSISDN Prefix Range Table.

Example

The following command specifies **table 1** with **round-robin** algorithm to select the rows with host name for E-PDF in Diameter host table.

```
diameter host-select table 1 algorithm round-robin
```

diameter origin endpoint

This command binds the origin endpoint configured in Context Configuration mode to the IMS Authorization service for Diameter Policy Control Application (DPCA).

Product

All

Privilege

Security Administrator, Administrator

Syntax

diameter origin endpoint *endpoint_name*

no diameter origin

endpoint *endpoint_name*

endpoint_name is the Diameter endpoint configured in Context Configuration Mode to bind with IMS authorization service, and must be an alpha/numeric string of 1 through 63 characters in length.

no

Removes the binding of Diameter origin endpoint with IMS Authorization service.

Usage

Use this command to bind a configured Diameter origin endpoint to the IMS Authorization service for DPCA. This IMS authorization service searches all system contexts until it finds one with a matching Diameter origin endpoint name specified.

Example

The following command binds a configured endpoint named test to the IMS authorization service:

```
diameter origin endpoint test
```

diameter request-timeout

This command configures the request-timeout setting for Diameter-IMSA Gx interface.

Product

GGSN, P-GW

Privilege

Security Administrator, Administrator

Syntax

diameter request-timeout *timeout*

default diameter request-timeout

timeout

Specifies the timeout period in seconds.
timeout must be an integer from 1 through 300.
Default: 10 seconds

default

Applies the default setting for this command.

Usage

Use this command to configure the request-timeout setting for Diameter-IMSA Gx interface.

Example

The following command configures the Diameter request-timeout setting to *20* seconds:

```
diameter request-timeout 20
```

diameter update-dictionary-avps

This command enables dictionary control of the AVPs that need to be added based on the version of the specification to which the PCEF is compliant with.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
diameter update-dictionary avps { 3gpp-r8 | 3gpp-r9 }

{ default | no } diameter update-dictionary avps
```

default | no

Configures this command with the default setting.
The default behavior is that R9 support will not be indicated as part of Supported-Features AVP in a R7/R8 dictionary and R8 support will not be indicated as part of Supported-Features AVP in a R7 dictionary.

3gpp-r8

Specifies to select the 3GPP Rel. 8 AVPs for encoding.

3gpp-r9

Specifies to select the 3GPP Rel. 9 AVPs for encoding.

Usage

Important: This command is applicable only to Diameter dictionaries that support standard based volume reporting over Gx feature.

Use this command to encode the AVPs in the dictionary based on the release version of the specification to which the PCEF is compliant with.
Release 12.0 onwards, if a 3GPP Rel. 7 based dictionary is already configured with **diameter dictionary dpca-custom4** command, and then if the **diameter update-dictionary-avps 3gpp-r9** command is applied, the Supported-Features AVP with feature bit 1 being set will be sent in the CCR-I to indicate that 3GPP Rel. 9 AVPs are also supported.
Both **default** and **no** command have the same behavior, as if the CLI command is not configured. Hence, in the output of **show configuration verbose** command, the **default** and **no** command is shown as **no diameter update-dictionary-avps**.
This CLI command when configured results in behavioral changes as indicated in the following table.

Possible Upgrade Scenarios	Behavior
3GPP Rel. 7 based dictionary upgraded to 3GPP Rel. 9 For example: **diameter dictionary dpca-custom4** **diameter update-dictionary-avps 3gpp-r9**	In the CCR-I, Supported-Features AVP will be encoded with value 2 for the Feature-List AVP. [V] [M] Supported-Features: [M] Vendor-Id: 10415 [V] [M] Feature-List-ID: 1 [V] [M] Feature-List: 2 The Feature-List AVP value suggest that it is 3GPP Rel. 9 compliant. But, it is not fully complaint to 3GPP Rel. 9. In the current release, for this upgrade scenario (3GPP Rel. 7 to 3GPP Rel. 9), only volume reporting related AVPs mentioned in the 3GPP Rel. 9 will be supported.
3GPP Rel. 7 based dictionary upgraded to 3GPP Rel. 8 For example: **diameter dictionary dpca-custom4** **diameter update-dictionary-avps 3gpp-r8**	In the CCR-I, Supported-Features AVP will be encoded with value 1 for the Feature-List AVP. [V] [M] Supported-Features: [M] Vendor-Id: 10415 [V] [M] Feature-List-ID: 1 [V] [M] Feature-List: 1 The Feature-List AVP value suggest that it is 3GPP Rel. 8 compliant. But, it is not fully complaint to 3GPP Rel. 8. In the current release, for this upgrade scenario (3GPP Rel. 7 to 3GPP Rel. 8), none of the features mentioned in 3GPP Rel. 8 will be supported.
3GPP Rel. 8 based dictionary upgraded to 3GPP Rel. 9 For example: **diameter dictionary r8-gx-standard** **diameter update-dictionary-avps 3gpp-r9**	In the CCR-I, value for the Feature-List AVP in the Supported-Features AVP will be 2. [V] [M] Supported-Features: [M] Vendor-Id: 10415 [V] [M] Feature-List-ID: 1 [V] [M] Feature-List: 2 The Feature-List AVP value suggest that it is 3GPP Rel. 9 compliant. But, it is not fully complaint to 3GPP Rel. 9. Currently for this upgrade scenario (3GPP Rel. 8 to 3GPP Rel. 9), only volume reporting related AVPs mentioned in 3GPP Rel. 9 will be supported.

Example

The following command enables encoding of AVPs in the dictionary based on 3GPP Rel. 9:

```
diameter update-dictionary-avps 3gpp-r9
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

event-report-indication

This command enables event report indication.

Product

P-GW

Privilege

Security Administrator, Administrator

Syntax

```
event-report-indication { all | pgw-trace-control | qos-change | rai-change | rat-change
| sgsn-change | ue-timezone-change | user-loc-change } [ pgw-trace-control ] [ qos-change
] [ rai-change ] [ rat-change ] [ sgsn-change ] [ ue-timezone-change ] [ user-loc-change
]

[ default | no ] event-report-indication
```

all | pgw-trace-control | qos-change | rai-change | rat-change | sgsn-change | ue-timezone-change | user-loc-change

Specifies which types of changes will trigger an event report from the PCRF.

- **all**: all triggers
- **pgw-trace-control**: P-GW trace control change trigger
- **qos-change**: QoS change trigger
- **rai-change**: RAI change trigger
- **rat-change**: RAT change trigger
- **sgsn-change**: SGSN change trigger
- **ue-timezone-change**: UE time zone change trigger
- **user-loc-change**: User location change trigger

default | no

Disables event report indication.

Usage

Use this command to determine what type of event changes are reported from the PCRF.

Example

The following command enables event report indication for all triggers.

```
event-report-indication all
```

event-update

This command configures sending usage information in event updates.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
event-update send-usage-report [ reset-usage ]

[ default | no ] event-update
```

default

Configures the default setting for this command.
Default: Usage report is not sent in event update.

no

Disables sending usage report in event update.

send-usage-report

Specifies to send volume usage report in event update.

reset-usage

Specifies to reset the usage at PCEF after reporting in event update.

Usage

Use this command to send volume usage information when an event change is reported to the PCRF in a CCR-U message.

Example

The following command specifies to send volume usage report in event updates to the PCRF:

```
event-update send-usage-report
```

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

failure-handling

This command configures Diameter failure handling behavior.

Product

All

Privilege

Security Administrator, Administrator

Syntax

In Release 8.0:

failure-handling { continue | retry-and-terminate | terminate | diameter-result-code { any-error | *result_code* } ccfh { continue | retry-and-terminate | terminate } [cc-request-type { initial-request | terminate-request | update-request }] }

no failure-handling diameter-result-code { any-error | integer *result_code* } [cc-request-type { initial-request | terminate-request | update-request }]

In 8.1 and later releases:

failure-handling cc-request-type { any-request | initial-request | terminate-request | update-request } { diameter-result-code { any-error | *result_code* [to *end_result_code*] } } { continue | retry-and-terminate | terminate }

no failure-handling cc-request-type { any-request | initial-request | terminate-request | update-request } [diameter-result-code { any-error | *result_code*[to *end_result_code*] }]

no

Disables previous failure-handling configuration.

continue

Specifies that in the event of a failure the user session continues. DPCA/Diameter will make periodic request and/or connection retry attempts and/or will attempt to communicate with a secondary peer depending on the peer config and session-binding setting.

retry-and-terminate

Specifies that in the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.

terminate

Specifies that in the event of a failure the user session be terminated.

diameter-result-code { any-error | *result_code* [to *end_result_code*] }

Specifies failure handling behavior for any/specific result-code(s) to identify the type of failure and failure handling action for specific credit control request type.

any-error: Specifies failure handling behavior for those result-codes for which failure-handling behavior has not been specified.
result_code: Specifies a Diameter failure result code. *result_code* is the code returned for a failure handling action and must be an integer from 3000 through 4999.
to *end_result_code*: Use to specify a range of Diameter failure result codes. *end_result_code* must be an integer from 3000 through 4999, and must be greater than *result_code*.

continue | retry-and-terminate | terminate

As in 8.1 and later releases.
Specifies the credit control failure handling action.

- **continue**: In the event of a failure the user session continues. DPCA/Diameter will make periodic request and/or connection retry attempts and/or will attempt to communicate with a secondary peer depending on the peer config and session-binding setting.
- **retry-and-terminate**: In the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.
- **terminate**: In the event of a failure the user session is terminated.

ccfh { continue | retry-and-terminate | terminate }

As in 8.0 release:
Specifies the credit control failure handling (CCFH) action with or without credit control request type.

- **continue**: In the event of a failure the user session continues. DPCA/Diameter will make periodic request and/or connection retry attempts and/or will attempt to communicate with a secondary peer depending on the peer config and session-binding setting.
- **retry-and-terminate**: In the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.
- **terminate**: In the event of a failure the user session is terminated.

cc-request-type

As in 8.0 release:
This optional keyword defines the type of credit control request with failure result code and credit control failure handling action for a session.

- **any-request**: Specifies the request type as any request for a new session.
- **initial-request**: Specifies the request type as initial request for a new session.
- **terminate-request**: Specifies the request type as terminate request for a session.
- **update-request**: Specifies the request type as update request for an active session.

Usage

Use this command to configure the Diameter Policy Control Application (DPCA) failure handling behavior. When an unknown rulebase comes in CCA, changing of rulebase and failure handling is managed in the following manner:

- If the new and existing rulebases have the same CCA policy, then switch to the new rulebase is successful.
- If the new rulebase is valid and has CCA-enabled, in CCA-Initial/Update request, switch to the new rulebase is successful.

- If the new rulebase is valid and does NOT have CCA enabled, whereas the existing rulebase has credit enabled, or vice versa, in CCA-Initial/Update request:
  - CCFH-Continue: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  - CCFH-RETRY&TERMINATE: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  - CCFH-TERMINATE: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
- If the new rulebase is invalid, in CCA-Initial/Update request:
  - CCFH-Continue: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  - CCFH-RETRY&TERMINATE: Terminates on successful CCA-T, or terminates after successful/failed retry to secondary.
  - CCFH-TERMINATE: Terminates on successful/failed CCR-T to Primary.

The default failure handling behavior is:
failure-handling diameter-result-code any-error ccfh terminate

Example

The following command sets the DPCA failure handling to **retry-and-terminate** and return a result code of *3456* for credit control request type **initial-request**:
As in 8.0 release:

```
failure-handling diameter-result-code 3456 ccfh retry-and-terminate cc-request-type initial-request
```

As in 8.1 and later releases:

```
failure-handling cc-request-type initial-request diameter-result-code 3456 retry-and-terminate
```

li-secret

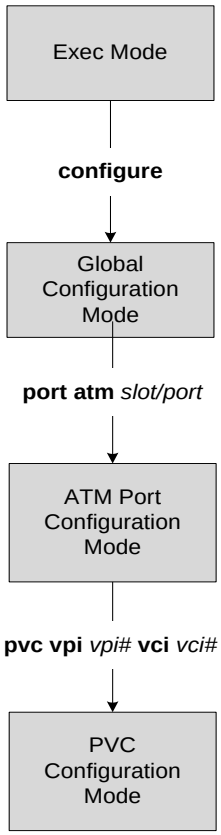
Refer to the *Cisco ASR 5000 Lawful Intercept Configuration Guide* for a description of this command.

Chapter 234
PVC Configuration Mode Commands

The Permanent Virtual Connection (PVC) configuration mode commands bind IP interfaces or SS7-Frame Relay links a PVC as well as configure PVC operational parameters for a specific port.

In this mode, the prompt line should appear similar to:

```
[local]hostname(config-port-<slot#>/<port#>-pvc-<pvc_num>/<vci_num>)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, version, and installed license(s).

bind

This command binds an IP interface or an SS7 link to the PVC.

Important: Prior to attempting the binding, the interface and context or the SS7 routing information and link must have been configured.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] bind { interface *interface_name context_name* **| link ss7-routing-domain** *rd_id* **linkset-id** *id* **link-id** *id* **}**

no

Removes the binding from the configuration.

interface_name

Defines the name of the virtual interface to be bound to the PVC. *interface_name:* Must be a unique string consisting of 1 to 79 alphanumeric characters.

context_name

Specifies the name of the context to be bound to the virtual interface. *context_name:* Must be a unique string consisting of 1 to 79 alphanumeric characters.

ss7-routing-domain *rd_id*

Identifies a specific SS7 routing domain. *rd_id* must be an integer from 1 to 12

linkset-id *id*

Identifies a specific linkset within the routing domain. *id*: must be an integer from 1 to 33

link-id *id*

Identifies a specific link within the linkset. *id*: must be an integer value 1 - 16

Usage

Use this command to bind the PVC to an interface or a specific link.

Example

Use a command similar to the following to bind a PVC to a link ID #2:

```
bind ss7-routing-domain 1 linkset-id 23 link-id 2
```

encapsulation aal5

Specify the data encapsulation type for the ATM adaptation layer 5 (AAL5) frames for the PVC.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
encapsulation aal5 { llc-snap | vc-mux }
```

llc-snap

Frames protocol is identified in the AAL5 using logical link control (LLC) encapsulation.

vc-mux

Frames are not encapsulated and use virtual circuit multiplexing (VC-MUX) to identify the protocols used for the AAL5 frames.

Usage

Use this command to identify the protocol type for the circuit.

Example

```
encapsulation aal5 vc-mux
```

end

Exits the PVC configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the PVC configuration mode and returns to the ATM port configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Return to the port configuration mode.

shaping

Specify the type of traffic shaping (rates) for this PVC.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

shaping { cbr pcr *prc_num* **| ubr pcr** *prc_num* **| ubr+ pcr** *prc_num* **mrc** *mrc_num* **| vbr pcr** *prc_num* **scr** *src_num* **mbs** *mbs_num* **}**

cbr

Constant bit rate
pcr - peak cell rate = cells per second
prc_num: Must be an integer from 75 to 1412830

ubr

Unspecified Bit Rate
pcr - peak cell rate = cells per second
prc_num: Must be an integer from 75 to 1412830

ubr+

Unspecified Bit Rate with Minimum Cell Rate.
The PCR and MCR values should be set to maintain the following relationship: PCR >= (MCR + minRate), where the current recomment minRate is 75.
pcr - peak cell rate = cells per second
prc_num: Must be an integer from 75 to 1412830
mcr - minimum cell rate
mrc_num: Must be an integer from 75 to 1412830

vbr

Variable Bit Rate, NRT (not real time) type.
The PCR and MCR values should be set to maintain the following relationship: PCR >= (MCR + minRate), where the current recomment minRate is 75.
pcr - peak cell rate = cells per second
prc_num must be an integer from 75 to 1412830
scr - sustained cell rate
src_num must be an integer from 75 to 1412830
mbs - maximum burst size
mbs_num must be an integer from 75 to 1412830

Usage

Use this command to configure the shaping for egress traffic on this PVC.

Example

shaping cbr pcr *56000*

shutdown

Disables/enables traffic over the current VLAN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
shutdown

no shutdown
```

no

Enables the VLAN. When omitted the VLAN is non-functional.

Usage

Enables/ Disables specified VLAN.
This command is necessary to bring a VLAN into service by enabling it via the **no** keyword.

Example

To disable a VLAN from sending or receiving network traffic use the following command:

```
shutdown
```

To enable a VLAN use the following command:

```
no shutdown
```

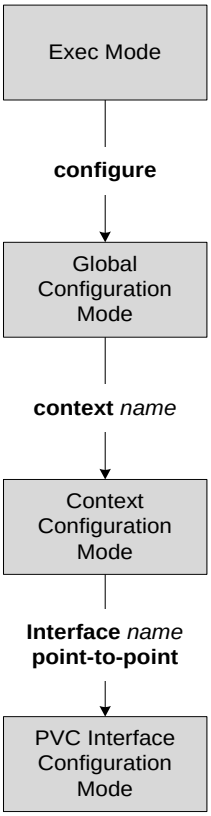
Chapter 235
PVC Interface Configuration Mode Commands

The PVC (permanent virtual connection) Interface configuration mode is used to create and manage the IP parameters for PVC interface(s) associated with an OLC (ATM-type) for a specific context.

In this mode, the prompt line should appear similar to:

```
[<context_name>]hostname<config-if-pvc)#
```

All configuration information specified with these commands is displayed using the Exec mode.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

description

Defines descriptive text to provide useful information about the current interface.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

description *text*

no description

no

Erases the port's description from the configuration file.

text

text: Must be a string of 1 to 79 alphanumeric characters with no spaces or a string within double quotes that includes printable characters. The description is case-sensitive.

Usage

Set the description to provide helpful information, for example the port's primary function, services, end users. Define any information, the only limit is the number of characters, 79.

Example

description *"PVC12 connects server 1 to home office."*

end

Exits the PVC interface configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Change the mode back to the Exec mode.

exit

Exits the interface configuration mode and returns to the context configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the context configuration mode.

ip

The commands in this section are used to configure the IP parameters for the PVC interface.

Important: Before configuring the OSPF parameters in this section, you need to enable OSPF using the router command and OSPF configuration sub-mode commands accessed in the Context configuration mode and documented in the Context Configuration Mode chapter of this Command Line Interface Reference.

ip access-group

This command identities the access control list (ACL to be associated with this PVC interface in this context.

Important: Prior to using this command, the access list must be created for this context with the **ip access-list** command in the Context configuration mode and then the ACL must be configured using the commands described in CLI chapter ACL Configuration Mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ip access-group *name* **{ in | out }**

no ip access-group *name* **{ in | out }**

no

Indicates the specified access group to be removed from the access list.

name

Specifies the access control list (ACL) rule to be added or removed from the group.
name: Must be a string of 1 to 79 alphanumeric characters with no spaces.

Important: Up to 8 ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128 rule limit for the interface.

in | out

in: Specifies list is for in-bound access control.
out: Specifies the list is for out-bound access control.

Important: Even though "in" or "out" can be specified, context-level ACL rules are automatically applied to both directions.

Usage

Use this command to add IP access lists configured for the same context to an IP access-group. The list can be configured to apply to all inbound and/or outbound traffic.

Example

The following adds ACL access-list-1 to the IP access-group associated with this PVC for this context.

```
ip access-group access-list-1 in
```

ip address

Defines the primary IP address and the network mask to be associated with this PVC interface for this context. This command can also be used to configure the secondary IP address.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ip address *ip_address ip_mask* **[secondary]**

no ip address *ip_address*

no

Removes the IP address information for this PVC from the configuration. It is not necessary to include the subnet mask with the command.
The command must first be issued with the secondary IP address if one exists and then re-issued with the primary IP address.

address *ip_address ip_mask*

Configures the IP address and the network mask for this PVC interface. The first time this command is entered, it automatically defines the primary IP address for this interface.
ip_address and *ip_mask* must be specified using the standard IPv4 or IPv6 dotted decimal notation.

secondary

secondary: Including this keyword indicates the IP address and subnet mask being defined are to be used as the secondary IP address for this PVC interface. This is referred to as multi-homing of the interface.

Usage

Configures or deletes the IPv4 or IPv6 addresses and subnet mask to be associated with this PVC.

Example

The following configures the secondary IP address to associate with the interface.

```
ip address 131.2.3.4 255.255.255.0  secondary
```

The following set of commands removes the primary IP address from the PVC interface configuration for this context.

```
no ip address secondary address

no ip address primary address
```

ip mtu

Configures the maximum transmission unit (MTU) to be supported on this interface.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ip mtu *value*

no ip mtu

no

Disables and/or restores the option to the system default.

mtu *value*

Configures the maximum transmission unit in octets.
value: Enter an integer between 576 and 1600. Default is 1500.

Usage

Change the maximum transmission unit size to 1300.

Example

ip mtu *1300*

ip ospf authentication-key

This command configures the password or key to be used for OSPF (Open Shortest Path First) authentication with neighboring routers.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ip ospf authentication-key [encrypted] password *auth_key*

no ip ospf authentication-key

no

Deletes the authentication key.

encrypted

Enter this keyword if you are pasting a previously encrypted authentication key into the **password** *auth_key* for this command.

password*auth_key*

auth_key is a string variable, from 1 through 16 alphanumeric characters, that denotes the authentication key (password). This variable is entered in clear text format.

Usage

Use this command to set the authentication key used when authenticating with neighboring routers.

Example

To set the authentication key to 123abc, use the following command;

```
ip ospf authentication-key password 123abc
```

Use the following command to delete the authentication key;

```
no ip ospf authentication-key
```

ip ospf authentication-type

This command configures the OSPF authentication method to be used with OSPF neighbors over the logical interface.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
ip ospf authentication-type { message-digest | null | text }

no ip ospf authentication-type { message-digest | null | text }
```

no

Disable this function.

message-digest

Set the OSPF authentication type to use the message digest (MD) authentication method.

null

Set the OSPF authentication type to use no authentication, thus disabling either MD or clear text methods.

text

Set the OSPF authentication type to use the clear text authentication method.

Usage

Use this command to set the type of authentication to use when authenticating with neighboring routers.

Example

To set the authentication type to use clear text, enter the following command;

```
ip ospf authentication-type text
```

ip ospf cost

This command configures the cost associated with sending a packet over this logical interface.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ip ospf cost *value*

no ip ospf cost

no

Disable this function.

value

Default: 10
The cost to assign to OSPF packets. This must be an integer from 1 through 65535.

Usage

Use this command to set the cost associated with routes from the interface.

Example

Use the following command to set the cost to 20;

```
ip ospf cost 20
```

Use the following command to disable the cost setting;

```
no ip ospf cost
```

ip ospf dead-interval

This command configures the dead-interval and the delay time in seconds, for OSPF communications.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ip ospf dead-interval *value*

no ip ospf dead-interval

no

Deletes the value set and returns the value to its default.

value

The interval, in seconds, that the router should wait. During this interval, if no packets are received then the system considers the neighboring router to be off-line. This interval is typically 4 times the duration of the hello-interval.
value must be an integer from 1 through 65535. Default: 40

Usage

Use this command to set the dead-intervals or delays for OSPF communications.

Example

To set the dead-interval to 100, use the following command;

ip ospf dead-interval *100*

To delete the setting for the dead-interval and reset the dead-interval value to its default of 40, use the following command'

no ip ospf dead-interval

ip ospf hello-interval

This command configures the delay time in seconds, for OSPF hello interval.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ip ospf hello-interval *value*

no ip ospf hello-interval

no

Deletes the value set and returns the value to its default.

value

The interval, in seconds, between sending hello packets. This value is typically set to be 1/4 of the value of the **dead-interval**.
value must be an integer from 1 through 65535. Default: 10

Usage

Use this command to set the delays for the hello-interval.

Example

To set the hello-interval to 25, use the following command;

```
ip ospf hello-interval 25
```

To delete the setting for the hello-interval and reset the hello-interval value to its default of 10, use the following command'

```
no ip ospf hello-interval
```

ip ospf message-digest-key

This command enables the use of MD5-based OSPF authentication.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ip ospf message-digest-key *key_id* **md5 [encrypted] password** *authentication_key*

no ip ospfmessage-digest-key *key_id*

no

Deletes the key.

message-digest-key key_id

Specifies the key identifier number. key_id must be an integer from 1 through 255.

encrypted

Use this if you are pasting a previously encrypted authentication key into the CLI command.

password *authentication_key*

The password to use for authentication. *authentication_key* is a string variable, from 1 through 16 alphanumeric characters, that denotes the authentication password. This variable is entered in clear text format.

Usage

Use this command to create an authentication key that uses MD5-based OSPF authentication.

Example

To create a key with the ID of 25 and a password of 123abc, use the following command;

```
ip ospf message-digest-key 25 md5 password 123abc
```

To delete the same key, enter the following command;

```
no ip ospf message-digest-key 25
```

ip ospf network

Configures the OSPF network type.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ip ospf network { broadcast | non-broadcast | point-to-multipoint | point-to-point }

no ip ospf network

no

Disable this function.

broadcast

Sets the network type to broadcast.

non-broadcast

Sets the network type to non-broadcast multi access (NBMA).

point-to-multipoint

Sets the network type to point-to-multipoint.

point-to-point

Sets the network type to point-to-point.

Usage

Use this command to specify the OSPF network type.

Example

To set the OSPF network type to broadcast, enter the following command;

```
ip ospf network broadcast
```

To disable the OSPF network type, enter the following command;

```
no ip ospf network
```

ip ospf priority

This command designates the OSPF router priority.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ip ospf priority *value*

no ip ospf priority *value*

no

Disable this function.

value

The priority value to assign. This must be an integer from 0 through 255.

Usage

Use this command to set the OSPF router priority.

Example

To set the priority to 25, enter the following command:

```
ip ospf priority 25
```

To disable the priority, enter the following command:

```
no ip ospf priority
```

ip ospf retransmit-interval

This command configures the retransmit-interval and the delay time in seconds, for OSPF communications.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ip ospf dead-interval *value*

no ip ospf dead-interval

no

Deletes the value set and returns the value to its default.

value

The interval, in seconds, between LSA (Link State Advertisement) retransmissions.
value must be an integer from 1 through 65535. Default: 5

Usage

Use this command to set the retransmit-intervals or delays for OSPF communications.

Example

To set the dead-interval to 25, use the following command;

ip ospf retransmit-interval *25*

ip ospf transmit-delay

This command configures the transmit-delay the OSPF communications parameters.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ip ospf transmit-delay *value*

no ip ospf transmit-delay

no

Deletes the value set and returns the value to its default.

transmit-delay *value*

The interval, in seconds, that the router should wait before transmitting a packet.
value must be an integer from 1 through 65535. Default: 1

Usage

Use this command to set the transmit-delay.

Example

To set the transmit delay to 5 seconds, use the following command;

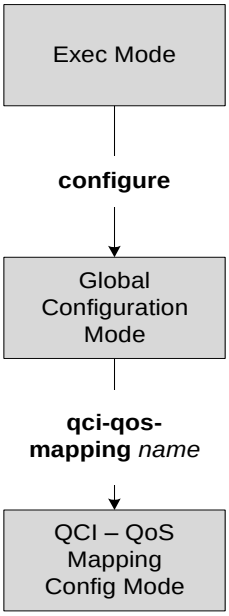
```
ip ospf transmit-delay 5
```

To delete the setting for the transmit-delay or reset the transmit-delay value to its default of 1, use the following command'

```
no ip ospf transmit-delay
```

Chapter 236
QCI - QoS Mapping Configuration Mode Commands

The QoS Class Index (QCI) to QoS Mapping Configuration Mode is used to map QoS Class Indexes to enforceable QoS parameters. Mapping can occur between the RAN and the Serving Gateway (S-GW), the Mobility Management Entity (MME), and/or the PDN Gateway (P-GW) in an LTE network or between the RAN and the eHRPD Serving Gateway (HSGW) in an eHRPD network.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

qci

Creates and maps QCI values to enforceable QoS parameters.

Product

HSGW, P-GW, S-GW

Privilege

Administrator

Syntax

qci *num* **[delay-class** *num* **precedence-class** *num* **reliability-class** *num* **[downlink | uplink]]**

qci *num* **[downlink { encaps-header { copy-inner | dscp-marking** *hex* **} | user-datagram dscp-marking** *hex* **[encaps-header { copy-inner | dscp-marking** *hex* **}] }]**

qci *num* **[gbr [delay-class | downlink | max-packet-delay | traffic-policing | uplink]]**

qci *num* **[max-packet-delay** *num* **max-error-rate** *num* **[downlink | uplink]]**

qci *num* **[non-gbr [delay-class | downlink | max-packet-delay | traffic-policing | uplink]]**

qci *num* **[traffic-policing interval** *interval* **[delay-class | downlink | max-packet-delay | uplink]]**

qci *num* **[uplink { encaps-header { copy-inner | dscp-marking** *hex* **} | user-datagram dscp-marking** *hex* **[encaps-header { copy-inner | dscp-marking** *hex* **}] }]**

[default | no] qci *num*

Important: The optional keywords associated with each of the initial optional keywords are abbreviated in the syntax examples above for clarity. Refer to the definitions below for the full keyword paths and associated descriptions for each keyword string in this command.

default

Resets the default values for the select QCI value.

no

Disables the selected QCI value.

num

Specifies the QCI value to be enabled. *num* must be an integer from 1 through 32.
QCI values of 1 through 9 are standard values. Only undefined values (10 through 32) can be defined.

Important: QCI values 1 through 9 are defined in *3GPP Specification TS 23.203 "Policy and charging control architecture"*.

delay-class *num* **precedence-class** *num* **reliability-class** *num*

delay-class *num*: Specifies the pre-release 8 value for configuring packet delay.
num must be an integer from 1 and 32.
precedence-class *num*: Specifies the pre-release 8 value for configuring packet precedence.
num must be an integer from 1 through 32.
reliability-class *num*: Specifies the pre-release 8 value for configuring packet reliability.
num must be an integer from 1 through 32.

downlink { encaps-header { copy-inner | dscp-marking *hex* **} | user-datagram dscp-marking** *hex* **[encaps-header { copy-inner | dscp-marking** *hex* **}] }**

Configures parameters for downlink traffic.
encaps-header: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.
user-datagram dscp-marking *hex*: Specifies that the UDP DSCP marking is to be defined by this keyword.
hex is expressed as a hexadecimal number from 0x00 through 0x3F.
{ copy-inner | dscp-marking *hex* **}**

- **copy-inner**: Specifies that the DSCP marking is to be acquired from the UDP headers within the encapsulation.
- **dscp-marking** *hex*: Specifies that the DSCP marking is to be defined by this keyword.

  hex ia expressed as a hexadecimal number from 0x00 through 0x3F.

gbr

Specifies that this QCI type is Guaranteed Bit Rate (GBR).

max-packet-delay *num* **max-error-rate** *num*

max-packet-delay *num*: Specifies the maximum packet delay (in milliseconds) that can be applied to the data with the QCI.
num must be an integer from 10 through 1000. Default is 10ms for QCI values greater than 9.
max-error-rate *num*: Specifies the maximum error loss rate of non-congestion related packet loss.
num must be an integer from 1 through 6, specifying 10-1 through 10-6. Default is 3 (or 10-3) for QCI values greater than 9.

Important: Defaults for QCI values less than 9 are defined in *3GPP Specification TS 23.203 "Policy and charging control architecture"*.

non-gbr

Specifies that this QCI type is non-Guaranteed Bit Rate (non-GBR).

traffic-policing interval *interval*

Specifies the traffic policing interval associated with the this QCI.
interval must be an integer from 1 through 100.

uplink { encaps-header { copy-inner | dscp-marking *hex* **} | user-datagram dscp-marking** *hex* **[encaps-header { copy-inner | dscp-marking** *hex* **}] }**

Configures parameters for uplink traffic.

encaps-header: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.

user-datagram dscp-marking *hex*: Specifies that the UDP DSCP marking is to be defined by this keyword.

hex is expressed as a hexadecimal number from 0x00 through 0x3F.

{ copy-inner | dscp-marking *hex* **}**

- **copy-inner**: Specifies that the DSCP marking is to be acquired from the UDP headers within the encapsulation.
- **dscp-marking** *hex*: Specifies that the DSCP marking is to be defined by this keyword.

  hex is expressed as a hexadecimal number from 0x00 through 0x3F.

Usage

Use this command to create and map QCI values to enforceable QoS parameters.

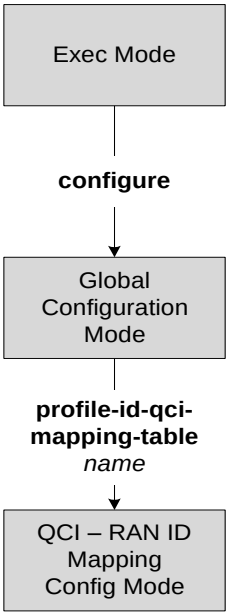
Example

The following command creates a QCI value of *15* and defines the uplink encapsulation header as using the DSCP marking from the encapsulated UDP header:

```
qci 15 uplink encaps-header copy-inner
```

Chapter 237
QCI - RAN ID Mapping Configuration Mode Commands

The QoS Class Index (QCI) Mapping Configuration Mode is used to map RAN profile IDs to QoS Class Indexes via the HRPD Serving Gateway (HSGW) in an eHRPD network.



end

Exits the current mode and returns to the Exec Mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

exit

Exits the current mode and returns to the previous mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the previous mode.

profile-id

Maps a QCI ID to a RAN profile ID and modifies data flow bit rate ranges.

Product

HSGW

Privilege

Administrator

Syntax

```
profile-id id qci num [ uplink { gbr rate [ mbr rate ] | mbr rate [ gbr rate ] } downlink
{ gbr rate [ mbr rate ] | mbr rate [ gbr rate ] ]

no profile-id id
```

no

Removes the specified profile ID entry from this map.

id

Specifies the profile ID to which a QCI ID will be mapped. *id* must be an integer value from 1 to 65535.

qci *num*

Specifies the QCI number to which the profile ID will be mapped. *num* must be an integer value from 1 to 255.

uplink

Specifies that the guaranteed bit rate (GBR) and/or maximum bite rate (MBR) setting that follow this keyword will be applied to the uplink data flow.

downlink

Specifies that the guaranteed bit rate (GBR) and/or maximum bite rate (MBR) settings that follow this keyword will be applied to the downlink data flow.

gbr *rate*

Specifies the guaranteed bit rate for the uplink or downlink data flow. *rate* must be an integer value from 0 to 4294967295.

mbr *rate*

Specifies the maximum bit rate for the uplink or downlink data flow. *rate* must be an integer value from 0 to 4294967295.

Usage

Use this command to map a QCI ID to a RAN profile ID and, optionally, modify data flow bit rate ranges.

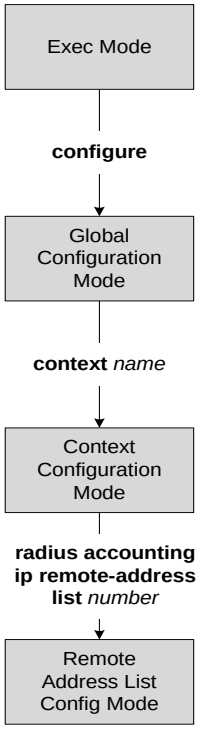
Example

The following command maps a QCI ID (*1*) to a profile ID (*10*) and sets the uplink guaranteed bite rate to *10000* and the downlink guaranteed bit rate to *20000*:

```
profile-id 10 qci 1 uplink gbr 10000 downlink gbr 20000
```

Chapter 238
Remote Address List Configuration Mode Commands

The Remote Address List Configuration Mode is used to configure address lists for the Remote Address-based Accounting feature on a per-context basis.



address

Configures addresses within a Remote Address List.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

[no] address *ip_address* **netmask** *subnet*

no

Removes a previously configured address.

ip_address

Specifies the IP address of the remote device.
ip_address is entered using IPv4 dotted-decimal or IPv6 colon-separated notation.

netmask *subnet*

Specifies the subnet mask of the remote device.
subnet is the netmask expressed in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use this command to configure remote address lists for use with the Remote Address-based accounting feature. A maximum of 10 address can be configured per list.

Example

The following command adds an IP address of *192.168.100.1* with a subnet mask of *255.255.255.0* to the list:

```
address 192.168.100.1 netmask 255.255.255.0
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

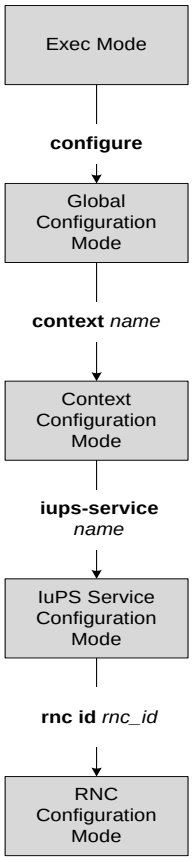
Use this command to return to the parent configuration mode.

Chapter 239
RNC Configuration Mode Commands

The RNC (radio network controller) configuration mode defines the parameters related to the SGSN connection with an RNC.

This mode is accessed from the IuPS Service configuration mode and the command prompt for this mode will appear similar to:

```
[<context_name>]hostname(config-ctx-iups-service-rnc)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

associate-gtpu-bind-address

This command defines the GTP-U loopback address and associates (binds) this address with a particular interface (non-loopback) address.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] associate-gtpu-bind-address *ip_address* **to-interface-address** *ip_address*

no

Removes the loopback address definition and interface association from the current RNC configuration.

ip_address

ip_address: Must be specified using the standard IPv4 dotted decimal notation.

Usage

Use this command to setup associations between loopback GTP-U addresses and a non-loopback addresses.

Example

Bind the GTP-U loopback address of *123.1.1.1* to interface address *222.1.1.1*:

```
associate-gtpu-bind-address 123.1.1.1 to-interface-address 222.1.1.1
```

description

This command defines an alphanumeric string that is intended to provide descriptive information about the radio network controller (RNC). This is used for operator reference only.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

description *string*

no description

no

Removes the description string from the current RNC configuration.

string

Specifies the alphanumeric string that is stored. must be from 1 through 255 alphanumeric characters. Strings with spaces must be enclosed in double-quotes. See the example below.

Usage

Use this command to set a description for reference by operators.

Example

The following command sets the description to identify a particular RNC and carrier in Uganda *"RNC1 Carrier2 Uganda"*:

```
description "RNC1 Carrier2 Uganda"
```

direct-tunnel

This command enables/disables the direct tunnel feature through the interface to the radio network controller (RNC).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
direct-tunnel not-permitted-by-rnc

default direct-tunnel
```

default

Sets the direct tunnel support on RNC to default mode; i.e. enabling direct tunnel.

not-permitted-by-rnc

Default: enabled
Disables the direct-tunnel support on radio network controller (RNC).

Usage

Use this command to disable/enable the direct-tunnel function through the interface to the RNC.

Example

Following command disables the direct tunnel support to the RNC:

```
direct-tunnel not-permitted-by-rnc
```

dual-address-pdp

This command enables the SGSN to work with an RNC with functioning dual address (IPv4v6) bearer support capability. By default, it is assumed that the RNC does not support dual PDP-type addressing.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
dual-address-pdp { not-supported | supported }

default dual-address-pdp
```

default

Resets the SGSN to function with an RNC that is not supporting dual PDP addressing.

not-supported

Default
Enables the SGSN to work with an RNC that does not support dual PDP-type addressing. It allows a single address bearer PDP-type to be activated with a configured PDP-type.

supported

Enables the SGSN to work with an RNC that does support dual PDP-type addressing.

Usage

This command enables the SGSN to support dual PDP-type addressing (IPv4v6) per RNC.
For a dual PDP context to be activated, the RNC should support the PDP-type IPv4v6 in the RAB assignment request. For an RNC that does support the dual PDP-type addressing, use this command to change the default configuration and to configure the SGSN to work with the RNC's dual address bearer support capability.
If the RNC does not support this functionality, then the **default** form of this command should be configured to enable the SGSN to activate a single-address bearer PDP context even if (1) the UE requests PDP type IPv4v6 and if (2) the subscription allows this PDP type. The single address bearer PDP type will be activated with a configured PDP type.
When a UE moves from an RNC that supports dual PDP-type addressing to another RNC that does not support dual PDP-type addressing, then the SGSN will deactivate the PDP context. This is done because, even if we preserve the PDP contexts, the UE would be unaware of the preserved PDP context. This would lead to non-synchronized behavior in the network. So the SGSN deactivates the PDP context with cause code "reactivation-required" to ensure the UE, RNC, SGSN, and GGSN are in synch. As well, this gives the UE the opportunity to activate a PDP context again without dual bearers.
The **sgsn-rnc-no-dual-pdp-init-pdp-deact** disconnect reason is used to indicate that a PDP context has been deactivated because of roaming into an RNC that does not support this feature.

Important: For this configuration to function, support for dual PDP-type addressing must be enabled at the global level (the default). To confirm the functionality is enabled, issue the **show sgsn-mode** command from the Exec

mode. If the PDP-type addressing is not enabled, then refer to the instructions for the **dual-address-pdp** command in the *SGSN Global Configuration Mode Commands* section.

Example

Use the following command to enable dual PDP-type addressing with a supporting RNC:

```
dual-address-pdp supported
```

end

Exits the configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode to the Exec mode.

exit

Exits the current configuration mode and returns to the IuPS Service configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the previous configuration mode.

lac

This command identifies a Local Area Concentrator (LAC) and a Remote Area Concentrator (RAC) and associates them with this RNC definition.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] lac lac_id rac rac_id
```

no

Deletes the LAC and RAC information from the system configuration.

lac_id

A unique numeric identifier for the LAC associated with the RNC.
lac_id must be an integer between 1 and 65535.

rac_id

A unique numeric identifier for the RLAC associated with the RNC.
rac_id must be an integer between 1 and 255.

Usage

Creates an association with a specific LAC and RAC.

Example

Associate LAC *545* and RAC *23* with this RNC:

```
lac 545 rac 23
```

mbms

Configures RNC options for multimedia broadcast multicast service.

Important: This feature and command are currently under development and are not supported.

Product

SGSN

overload-action disable

This command maps an action to be taken if traffic reaches or exceeds defined levels.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

overload-action disable { activate | attach | auth-challenge | modify-request | paging-downlink-data | ptmsi-reallocation | service-request-data | sms } traffic-level *traffic-level*

[no | default] overload-action disable { activate | attach | auth-challenge | modify-request | paging-downlink-data | ptmsi-reallocation | service-request-data | sms }

no

Removes the defined overload action from configuration.

default

Resets the traffic level to the default level for the associated overload action.

activate traffic-level *traffic-level*

The system rejects new requests to activate PDP contexts if the defined traffic-level is exceeded.
traffic-level: An integer 1 to 15.
Default: 14

attach traffic-level *traffic-level*

The system rejects new requests for GPRS attach if the defined traffic-level is exceeded.
traffic-level: An integer 1 to 15.
Default: 15

auth-challenge traffic-level *traffic-level*

The system skips performing authentication challenges if the defined traffic-level is exceeded.
traffic-level: An integer 1 to 15.
Default: 4

modify-request *traffic-level*

The system rejects requests to modify a PDP context if the defined traffic-level is exceeded.
traffic-level: An integer 1 to 15.
Default: 12

paging-downlink-data traffic-level *traffic-level*

If the defined traffic-level is exceeded, then paging is not performed for data during downlinks if RABs are not available.

traffic-level: An integer 1 to 15.
Default: 11

ptmsi-reallocation traffic-level *traffic-level*

The system skips performing ptmsi-reallocation if the defined traffic-level is reached or exceeded.
traffic-level: An integer from 1 to 15.
Default: 4

service-request-data traffic-level *traffic-level*

The system rejects service requests to accept data and establish new RABs if the defined traffic-level is reached or exceeded.
traffic-level: An integer from 1 to 15.
Default: 10

sms traffic-level *traffic-level*

The system rejects SMS signaling if the defined traffic-level is reached or exceeded.
traffic-level: An integer 1 to 15.
Default: 8

Usage

This command defines traffic levels and the actions to take if traffic exceeds the defined levels. The command can be re-entered multiple times to create individual definitions for each type of traffic level and action.

Example

Use the following to instruct the system to reject service requests to establish new RABs if the traffic level reaches *3*:

```
overload-action disable service-request-data traffic-level 3
```

paging-non-searching-indication

This command instructs the SGSN to include the non-searching indicator flag in the page-request message.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
paging-non-searching-indication { non-searching | searching }

[ no | default ] paging-non-searching-indication
```

no | default

This is the default. Entering no or default with this command disables the inclusion of the flag.

non-searching

Set the non-searching-indication to non-searching in the page-request message.

searching

Set the non-searching-indication to searching in the page-request message.

Usage

Use this command to determine which type of search indicator flag will be included in the page-request message.

Example

Use this command to include the non-searching flag in page-request messages:

```
paging-non-searching-indication non-searching
```

pointcode

Configures the point code of the RNC.

The access protocol that is part of the IuPS Service configuration mode must be configured prior to defining the RNC's point code.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

pointcode *pt_code*

no pointcode

no

Deletes the RNC's point code information from the system configuration.

pt_code

Point code in dotted-decimal format :

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- string of 1 to 11 characters

Usage

Use this command to identify the point code of the associated RNC.

Example

Identify the pointcode for this RNC as *1.234.2*:

```
pointcode 1.234.2
```

pooled

Configure an RNC as either ‘pooled’ or ‘non-pooled’.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

pooled

[default | no] pooled

default | no

Entering either **default** or **no** returns the RNC configuration to the default ‘non-pooled’ state.

Usage

Each RNC, one-at-a-time, can be identified as ‘pooled’ -- as participating within an SGSN pool -- or ‘non-pooled’. Pooled RNCs can co-exist with non-pooled RNCs.

Example

Identify this RNC as being part of an SGSN pool:

```
pooled
```

rab-modify-procedure

This command configures how the RAB (radio access bearer) assignment procedure will be modified

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
rab-modify-procedure { normal-modify | release-and-establish }

default rab-modify-procedure
```

default

Returns the configuration to the default setting for this command parameter.

normal-modify

Selects the normal RAB modify procedure.

release-and-establish

Instructs the system to release and establish the RAB procedure.

Usage

Set the procedure to establish the radio access bearer (RAB).

Example

```
rab-modify-procedure normal-modify
```

ranap global-cn-id

This command configures the SGSN to use include the Global Core Network ID IE in the various messages.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
ranap global-cn-id { paging-request | relocation-request | reset-procedure | reset-resource-procedure } [ network-sharing selected-plmn ]

[ default | no ] ranap global-cn-id { paging-request | relocation-request }
```

default

Returns the configuration to the default setting and sends the common-plmn in the Global CN ID IE.

no

Disables sending the Global CN ID IE.

paging-request

Instructs the SGSN to send the Global CN ID IE in the Paging Request message.

relocation-request

Instructs the SGSN to send the Global CN ID IE in the Relocation Request message.

reset-procedure

Instructs the SGSN to send the Global CN ID IE in the Reset/Ack message.

reset-resource-procedure

Instructs the SGSN to send the Global CN ID IE in the Reset-Resource/Ack message.

network-sharing selected-plmn

Instructs the SGSN to send the selected-plmn in the Global CN ID IE *if* network sharing has been enabled.

Usage

Use this command to configure the SGSN to use 'selected-plmn' in the Global Core Network ID IE in various messages when network sharing is enabled.

Example

Use the following command to include the global-cn-id IE in a Paging Request with the common PLMN when network sharing is enabled :

```
default ranap global-cn-id paging-request
```

Use the following command to include global-cn-id IE in Relocation Request with the selected-plmn (assumes network sharing has been enabled):

```
ranap global-cn-id relocation-request network-sharing selected-plmn
```

ranap paging-area-id

This command configures the SGSN to use include the Paging Area ID IE in the Paging Request message.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
ranap paging-area-id paging-request [ network-sharing selected-plmn ]

[ default | no ] ranap paging-area-id paging-request [ network-sharing selected-plmn ]
```

default

Returns the configuration to the default setting and sends the common-plmn in the Paging Area ID IE.

no

Disables sending the Paging Area ID IE.

paging-request

Instructs the SGSN to send the Paging Area ID IE in the Paging Request message.

network-sharing selected-plmn

Instructs the SGSN to send the selected-plmn in the Paging Area ID IE *if* network sharing has been enabled.

Usage

Use this command to configure the SGSN to use 'selected-plmn' in the Paging Area ID IE in the Paging Request message when network sharing is enabled.

Example

Use the following command to include the paging-area-id IE in a Paging Request with the common PLMN when network sharing is enabled :

```
default ranap paging-area-id paging-request
```

Use the following command to include global-cn-id IE in Paging Request with the selected-plmn (assumes network sharing has been enabled):

```
ranap global-cn-id paging-request network-sharing selected-plmn
```

ranap paging-cause-ie

This command sets the paging cause value and either includes or suppresses the Paging Cause IE in responses to Paging Requests due to various sources. This command is available in releases 8.1 and higher.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ranap { paging-cause-ie { all | background-data [*value* **] | conversational-data [** *value* **] | gmm-signalling [** *value* **] | gs-signalling [** *value* **] | interactive-data [** *value* **] | sm-signalling [** *value* **] | sms-signalling [** *value* **] | streaming-data [** *value* **] }**

[default | no] ranap { paging-cause-ie { all | background-data | conversational-data | gmm-signalling | gs-signalling | interactive-data | sm-signalling | sms-signalling | streaming-data }

default

Resets the specific parameters value to default.

no

Suppresses the Paging Cause IE so that it is not included in responses to Paging Requests from respective sources.

all

Using **all** sets the action for the Paging Cause IE value for all paging due to all sources.

background-data [*value* **]**

Default: 3 (terminating background call)
Set the Paging Cause IE value for paging due to background data.
value : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

conversational-data [*value* **]**

Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to conversational data.
value : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

gmm-signalling [*value* **]**

Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to gmm-signaling.
value : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

gs-signalling [*value* **]**

Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to VLR Paging Request.

value : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

interactive-data [*value*]

Default: 2 (terminating interactive call)
Set the Paging Cause IE value for paging due to interactive data.
value : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

sm-signalling [*value*]

Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to SM signaling.
value : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

sms-signalling [*value*]

Default: 4 (terminating low priority signaling)
Set the Paging Cause IE value for paging due to SMS signaling.
value : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

streaming-data [*value*]

Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to streaming data.
value : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

Usage

This command can be used to set the value (meaning) of the Paging Cause IE included in responses to Paging Requests or it can be used to suppress the inclusion of the Paging Cause IE in the responses. These actions can be configured for paging for all sources or for a specified source.
The following values are applicable to all Paging Cause IEs:

- **0** - Terminating conversational call
- **1** - Terminating streaming call
- **2** - Terminating interactive call
- **3** - Terminating background call
- **4** - Terminating low priority signaling
- **5** - Terminating high priority signaling

Example

Use the following command to set Paging Cause value to *3* for paging due to GMM signaling without affecting cause values for other sources:

```
ranap paging-cause-ie gmm-signalling 3
```

Use the following command to suppress the Paging Cause IE from all Paging Requests to the RNC:

```
no ranap paging-cause-ie all
```

Either of the following commands will cause the Paging Cause IE to be included in Paging Requests with the default value for SM signaling without affecting the cause for other sources:

```
ranap paging-cause-ie sm-signalling
```

```
default ranap paging-cause-ie sm-signalling
```

ranap signalling-indication-ie

This command enables/disables the inclusion of the Signaling Indication IE in either or both the RAB Assignment Request and/or the Relocation Request RANAP messages.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
ranap signalling-indication-ie { rab-assignment-request [ relocation-request ] |
relocation-request [ rab-assignment-request ] }

no ranap signalling-indication-ie

default ranap signalling-indication-ie
```

no

Sets the configuration so that the SGSN never includes the IE.

default

Resets the configuration to the default - the SGSN includes the IE in the messages if preconditions are met (see Usage section).

rab-assignment-request | relocation-request

Including one or both of these keywords configures what type of RANAP message will include the IE.

Usage

The command enables the operator to determine whether the signalling indication information element is included in either or both the RAB Assignment Request and Relocation Request messages during the PDP context setup procedure.

For this command configuration to work so that the IE is included, two preconditions must be met:

- Received QoS traffic class for the context must be interactive
- Received QoS has a signalling indication value as optimized

When an RNC receives this IE, the RNC assumes that the customer is using IMS signaling and allocates massive amounts of bandwidth, potentially causing cell congestion. This command enables the operator to determine the usage of this IE which provides the operator with additional session management control.

Example

Use the following command to include the signalling indication IE in the RAB Assignment Request:

```
ranap signalling-indication-ie rab-assignment-request
```

ran-information-management

Use this command to inform the SGSN which RNC are capable of handling RAN information management (RIM) messages.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] ran-information-management
```

default

Resets the default so RIM is disabled.

no

Disables the RIM support in the configuration file.

Usage

By default, handling of RAN information management (RIM) messages is disabled. This command informs the SGSN which RNC are capable of handling RIM messages. This configuration only becomes 'operational' if the **ran-information-management** command is enabled in the SGSN global configuration mode. When RIM support is enabled on both the SGSN and the destination node, then all RIM PDUs are forwarded to the BSC/RNC. If RIM message handling is not enabled on both nodes, then the RIM PDUs are dropped silently.

Example

Use the following command to enable RIM support:

```
ran-information-management
```

Use the following command to disable RIM support that has been added to the configuration:

```
no ran-information-management
```

release-compliance

This command allows the SGSN to set support based on the RNC's 3GPP release compliance and to define per RNC QoS overrides.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

release-compliance { pre-release-7 | release-7 } [gbr-down *gbr_dn_val* **| gbr-up** *gbr_up_val* **| mbr-down** *mbr_dn_val* **| mbr-up** *mbr_up_val* **] +**

default release-compliance

default

Returns the configuration to the default value, **release-7**.

pre-release-7

Enables support for an RNC with capabilities compliant with releases prior to Release 7, such as HSPA in R6.

release-7

Enables support for RNC with capabilities compliant with 3GPP Release 7 or later, such as HSPA+ available in R7.

gbr-down *gbr_dn_val*

Defines a guaranteed kbps bit rate for downlink direction,

- options for **pre-release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000. Default cap is 16000.
- options for **release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000, 21000, 28000, 42000. See default cap information below.

gbr-up *gbr_up_val*

Defines a guaranteed kbps bit rate for uplink direction,

- options for **pre-release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000. Default cap is 16000.
- options for **release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000, 21000, 28000, 42000. See default cap information below.

mbr-down *mbr_dn_val*

Defines a maximum kbps bit rate for downlink direction,

- options for **pre-release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000. Default cap is 16000.

- options for **release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000, 21000, 28000, 42000. See default cap information below.

mbr-up *mbr_up_val*

Defines a maximum kbps bit rate for uplink direction,

- options for **pre-release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000. Default cap is 16000.
- options for **release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000, 21000, 28000, 42000. See default cap information below.

Usage

Use this command to match the 3GPP release support by the RNC. As the 3GPP releases each support differing data rate options - R6 supports HSPA and R7 supports HSPA+ - then selecting the compliance is a method of preforming data rate management on a per RNC basis.
Also use this command to set QoS capping overrides for each RNC separately. Default caps for Release 7 RNC will vary depending upon which overrides are set.

Important: Once caps are set for an RNC, if the RNC release level changes the capping remains the same until the QoS override values are changed for that RNC. Values do not automatically change to the default values appropriate for that release .

Example

Enable HSPA fallback to R6 compliance:

```
release-compliance pre-release-7
```

reset-resource

This command enables the operator to control message length by configuring the number of IuConIDs sent in each RANAP Reset Resource messages.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

reset-resource max-iuconid-per-msg *number*

default reset-resource max-iuconid-per-msg

default

Resets the number of Iu connection Ids included in the Reset Resource messages. Default is 250.

max-iuconid-per-msg *number*

Sets the number of Iu connection Ids to be included in the Reset Resource messages.
number: Integer from 1 to 250.
Default: 250

Usage

Id numbers for each Iu connection are included in the RANAP Reset Resource messages. Including this potentially long stream of numbers can make the message very long. With this command, the operator can control the size of the messages by controlling the number of Id messages included in the messages.

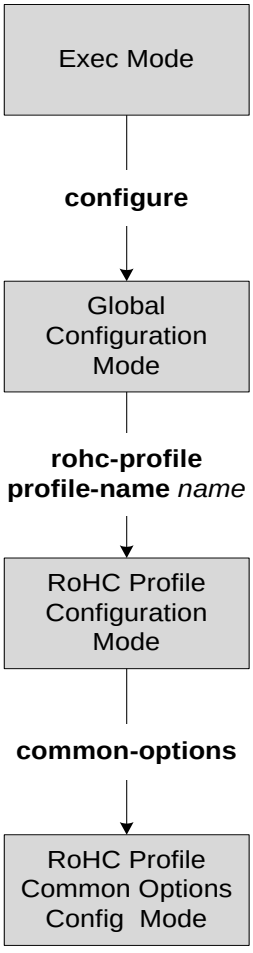
Example

Limit the number of Iu connection IDs to *30*:

```
reset-resource max-iuconid-per-msg 30
```

Chapter 240
RoHC Profile Common Options Configuration Mode Commands

The RoHC Profile Common Options Configuration Mode is used to set timers that, upon expiration, release robust header compression contexts.



delay-release-hc-context-timer

Sets a delay in releasing Robust Header Compression (RoHC) contexts allowing for context continuation during intra-gateway handoffs.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

delay-release-hc-context-timer *seconds*

no delay-release-hc-context-timer

no

Removes previously configured value for this command. No value disables the feature.

seconds

Specifies the number of seconds the system delays before releasing the header compression context as an integer from 0 to 65535.

Usage

Use this command to set a delay in releasing a header compression context. THis command is necessary when employing RoHC and mobility. Typically, when an RP connection is released, the header compression context is also released immediately. However, in mobility situations, such as intra-PDSN handoffs, the header compression context should be preserved. Adding a delay to cover the handoff time allows the context to be maintained.
A header compression context contains the compression/decompression configuration and statistics for the session.

Example

The following command sets the header compression release delay to 20 seconds:

```
delay-release-hc-context-timer 20
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

inactive-traffic-release-hc-context-timer

Sets an inactivity timer that is checked when inactivity is detected on an SO67 A10 bearer connection with negotiated RoHC parameters. When this timer expires, the header compression context is released.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

inactive-traffic-release-hc-context-timer *seconds*

no inactive-traffic-release-hc-context-timer

no

Removes previously configured value for this command. No value disables the feature.

seconds

Specifies the time, in seconds, the system waits for activity on the bearer channel before releasing the header compression context as an integer from 1 through 65535.

Usage

Use this command to set a timer that is started upon detecting inactivity on the bearer channel. Upon expiry, the header compression context is released. Enable this feature for more efficient memory utilization.

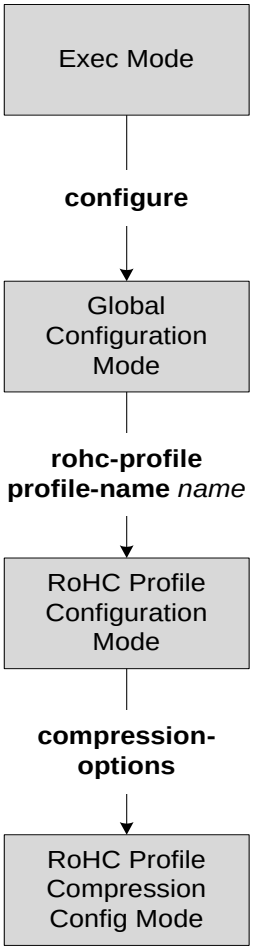
Example

The following command sets the bearer channel inactivity timer to 60 seconds:

```
inactive-traffic-release-hc-context-timer 60
```

Chapter 241
RoHC Profile Compression Configuration Mode Commands

The RoHC Profile Compression Configuration Mode is used to configure RoHC (Robust Header Compression) Compressor parameters. RoHC is not supported on GGSN.



Important: The availability of commands, keywords and variables in this mode are dependent on platform type, product version, and installed license(s).

context-timeout

Context timeout in seconds.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

context-timeout *seconds*

default context-timeout

default

Returns the command to its default value.

seconds

Specifies the context timeout value (in seconds) as an integer from 0 through 100.
Default: 20

Usage

Use this command to set the context timeout.

Example

The following command sets the context timeout to 10 seconds:

```
context-timeout-period 10
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

ipid-history-size

Specifies the number of IP-IDs of previously sent packets to store. An IP ID is a 16-bit header field that stores IPv4 Identification information.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

ipid-history-size *number*

default ipid-history-size

default

Returns the command to its default value.

number

Specifies the number of IP IDs to store as an integer from 1 through 32.
Default: 8

Usage

Use this command to set the number of IP IDs to store in the history.

Example

The following command sets the history size to 24 IP-IDs:

```
ipid-history-size 24
```

max-jitter-cd

Specifies the upper boundary of jitter expected on the communication channel between the compressor and decompressor.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

max-jitter-cd *num_ms*

default max-jitter-cd

default

Returns the command to its default value.

num_ms

Specifies the number of milliseconds for the maximum jitter setting as an integer from 0 through 999999999.
Default: 150

Usage

Use this command to set the maximum amount of jitter allowed on the communication channel between compressor and decompressor.

Example

The following command sets the jitter limit to 1000 ms (1 second):

```
max-jitter-cd 1000
```

max-sliding-window

Specifies the width of the sliding window for W-LSB (Windows-based Least Significant Bits) encoded values.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

max-sliding-window *size*

default max-sliding-window

default

Returns the command to its default value.

size

Specifies the size of the sliding window as an integer from 1 through 1000.
Default: 6

Usage

Use this command to set the size of the sliding window used to compute jitter for W-LSB encoded values.

Example

The following command sets the sliding window size to 500:

```
max-sliding-window 500
```

multiple-ts-stride

Enables or disables the use of repeated transmission of RTS_STRIDE for timer-based compression.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ no ] multiple-ts-stride
```

no

Disables the use of repeated transmission of RTS_STRIDE for time-based compression.

Usage

Use this command to enable or disable a gateway's ability to repeatedly transmit RTS_STRIDE for timer-based compression.

new-context-blocking-time

Specifies the time period in seconds for blocking the establishment of new contexts after the compressor has received a feedback reject.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

new-context-blocking-time *seconds*

default context-timeout

default

Returns the command to its default value.

seconds

Specifies the context blocking time (in seconds) as an integer from 0 through 100.
Default: 20

Usage

Use this command to set the context blocking time after the compressor has received a feedback reject.

Example

The following command sets the context blocking time to 10 seconds:

```
new-context-blocking-time 10
```

num-pkts-ts

Specifies the number packets per RTP timestamp (TS).

Product

HSGW, PDSN

Privilege

Administrator

Syntax

num-pkts-ts *num_pkts*

default num-pkts-ts

default

Returns the command to its default value.

num_pkts

Specifies the number of packets for the timestamp as an integer from 0 through 999.
Default: 6

Usage

Use this command to set the number of packets for each RTP timestamp (TS).

Example

The following command sets the number of packets per timestamp to 50:

```
num-pkts-ts 50
```

num-pkts-u-mode

Specifies the number of packets sent when operating in U-Mode (unidirectional mode).

Product

HSGW, PDSN

Privilege

Administrator

Syntax

num-pkts-u-mode *num_pkts*

default num-pkts-u-mode

default

Returns the command to its default value.

num_pkts

Specifies the number of packets sent in U-Mode as an integer from 0 through 999.
Default: 1

Usage

Use this command to set the number of packets sent when in U-Mode.

Example

The following command sets the number of packets for U-Mode to 50:

```
num-pkts-u-mode 50
```

num-updates-ir

Configures the number of IR (Initiation and Refresh state) updates.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

num-updates-ir *num_pkts*

default num-updates-ir

default

Returns the command to its default value of 4.

num_pkts

Specifies the number of IR updates as an integer from 0 through 999.
Default: 4

Usage

Use this command to set the number of IR updates.

Example

The following command sets the number of IR updates to 30:

```
num-updates-ir 30
```

optimistic-repeats

Specifies the number of repeated packets to send to the decompressor. For transition from the FO (First Order) to the SO (Second Order) state, the compressor should be confident that the decompressor has all the parameters needed to decompress according to a fixed pattern.The compressor obtains its confidence about decompressor status by sending several packets with the same information according to the lower compression state. If the decompressor receives any of these packets, it is in sync with the compressor.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

optimistic-repeats *num_pkts*

default optimistic-repeats

default

Returns the command to its default value.

num_pkts

Specifies the number of packets to repeat with the same information to assure synchronization with the decompressor.
num_pkts must be an integer from 0 through 10.
Default: 6

Usage

Use this command to set the number of packets to repeat to the decompressor to assure synchronization before transition states.

Example

The following command sets the number of repeated packets to 5:

```
optimistic-repeats 5
```

rtp-sn-p

Specifies the value of p in RTP SN (RTP Sequence Number) calculation. Least Significant Bits (LSB) encoding is used for header fields whose values are usually subject to small changes. With LSB encoding, the k least significant bits of the field value are transmitted instead of the original field value, where k is a positive integer. After receiving k bits, the decompressor derives the original value using a previously received value as reference (v_ref). The scheme is guaranteed to be correct if the compressor and the decompressor each use interpretation intervals as follows:

- In which the original value resides
- And in which the original value is the only value that has the exact same k least significant bits as those transmitted.

The interpretation interval can be described as a function:

f(v_ref, k). Let f(v_ref, k) = [v_ref - p, v_ref + (2^k - 1) - p]

Where p is an integer.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

rtp-sn-p *p_value*

default rtp-sn-p

default

Returns the command to its default value.

p_value

Specifies the value of p in the RTP SN calculation as an integer from 0 through 999.
Default: 6

Usage

Use this command to set the value for p when performing the RTP SN calculation.

Example

The following command sets the value of p to 100:

```
rtp-sn-p 100
```

rtp-sn-p-override

Enables an override of p in the RTP SN calculation. This is disabled by default.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default | no ] rtp-sn-p-override
```

default

Returns the command to its default value of disabled.

no

Disables overriding p in RTP SN calculation.

Usage

Use this command to enable an override of p in RTP SN calculation.

Example

The following command enables the override of p in the RTP SN calculation:

```
rtp-sn-p-override
```

rtp-time-stride

Sets the time interval used for one TS (RTP Time Stamp) stride. This interval is used when timer-based encoding is enabled.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

rtp-time-stride *num_ms*

default rtp-time-stride

default

Returns the command to its default value.

num_ms

Specifies the number of milliseconds to use for TS_STRIDE as an integer from 0 through 999999999.
Default: 20

Usage

Use this command to set the length of the TS_STRIDE in milliseconds.

Example

The following command sets TS_STRIDE to 100ms:

```
rtp-time-stride 100
```

rtp-ts-deviation

Sets the maximum percentage of deviation allowed for input RTP packets for timer-based compression.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

rtp-ts-deviation *percentage*

default rtp-ts-deviation

default

Returns the command to its default value of 25.

percentage

Specifies the maximum percentage of deviation allowed for input RTP packets for timer-based compression as an integer value from 0 through 100.
Default: 25

Usage

Use this command to set the maximum percentage of deviation allowed for input RTP packets for timer-based compression.

Example

The following command sets the percentage to 30:

```
rtp-ts-deviation 30
```

rtp-ts-stride

Specifies the amount by which TS (RTP time stamp) is incremented. This value is used for Scaled RTP TS encoding.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

rtp-ts-stride *num_ms*

default rtp-ts-stride

default

Returns the command to its default value of 160.

num_ms

Specifies the number of milliseconds to use incrementing TS as an integer from 0 through 999999999.
Default: 160

Usage

Use this command to set the amount by which TS is incremented for Scaled RTP TS encoding.

Example

The following command sets amount by which TS is incremented to 100ms:

```
rtp-ts-stride 100
```

sliding-window-ts

Sets the sliding window used to compute jitter.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

sliding-window-ts *size*

default sliding-window-ts

default

Returns the window to its default value of 4.

size

Specifies the size of the sliding window as an integer from 1 through 1000.
Default: 4

Usage

Use this command to set the size of the sliding window used to compute jitter for the current RoHC profile.

Example

The following command sets the sliding window size to 500:

```
sliding-window-ts 500
```

total-jitter-ipv4

Specifies the total jitter allowed after compression for IPv4.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

total-jitter-ipv4 *time*

default total-jitter-ipv4

default

Returns the command to its default value of 270.

time

Specifies the time interval to use (in milliseconds) as an integer from 0 through 999999999.
Default: 270

Usage

Use this command to set the jitter limit after compression.

Example

The following command sets the jitter after compression limit to 900 ms:

```
total-jitter-ipv4 900
```

total-jitter-ipv6

Specifies the total jitter allowed after compression for IPv6.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

total-jitter-ipv6 *time*

default total-jitter-ipv6

default

Returns the command to its default value 580.

time

Specifies the total jitter interval allowed (in milliseconds) as an integer from 0 through 999999999.
Default: 580

Usage

Use this command to set the jitter limit after compression.

Example

The following command sets the jitter after compression limit to 900 ms:

```
total-jitter-ipv6 900
```

unimode-timeout-to-fo-state

Specifies the time period in seconds before falling back to the FO (First Order) state.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

unimode-timeout-to-fo-state *num_ms*

default unimode-timeout-to-fo-state

default

Returns the command to its default value of 3.

num_ms

Specifies the timeout period (in seconds) as an integer from 0 through 10.
Default: 3

Usage

Use this command to set the timeout before falling back to the FO state when in Unimode.

Example

The following command sets the fall back timeout to 2 seconds:

```
unimode-timeout-to-fo-state 2
```

unimode-timeout-to-ir-state

Specifies the time period in seconds before falling back to the IR (Initiation and Refresh) state.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

unimode-timeout-to-ir-state *num_ms*

default unimode-timeout-to-ir-state

default

Returns the command to its default value of 5.

num_ms

Specifies the timeout period in seconds as an integer from 0 through 20.
Default: 5

Usage

Use this command to set the timeout before falling back to the IR state when in Unimode.

Example

The following command sets the fall back timeout to 3 seconds:

```
unimode-timeout-to-ir-state 3
```

use-calculated-rtp-time-stride

Overrides the configured value of rtp-time-stride with a calculated value.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default | no ] use-calculated-rtp-time-stride
```

default

Returns the command to its default value of enabled.

no

Disables the use of calculated RTP time stride override.

Usage

This command overrides the configured value of rtp-time-stride with a calculated value.

Example

The following command overrides the configured value of rtp-time-stride.

```
use-calculated-rtp-time-stride
```

use-calculated-rtp-ts-stride

Overrides the configured value of rtp-ts-stride with a calculated value.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

[default | no] use-calculated-rtp-ts-stride

default

Returns the command to its default value of enabled.

no

Disables the use of calculated RTP TS time stride override.

Usage

This command overrides the configured value of rtp-ts-stride with a calculated value.

Example

The following command overrides the configured value of rtp-ts-stride.

use-calculated-rtp-ts-stride

use-ipid-override

Enables or disables overriding the IP-ID (IPv4 Identification header field).

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default | no ] use-ipid-override
```

default

Returns the command to its default value of disabled.

no

Disables the IP-ID override.

Usage

Use this command to enable overriding of the IP-ID.

Example

The following command enables the IP-ID override feature:

```
use-ipid-override
```

The following command disables the IP-ID override feature:

```
no use-ipid-override
```

The following command also disables the IP-ID override feature:

```
default use-ipid-override
```

use-optimized-talkspurt

Enables or disables the use of optimized talkspurt.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default | no ] use-optimized-talkspurt
```

default

Returns the command to its default value of enabled.

no

Disables the use of optimized talkspurt.

Usage

Use this command to enable and disable the use of optimized talkspurt

Example

The following command enables the use of optimized talkspurt:

```
use-optimized-talkspurt
```

The following command disables the use of optimized talkspurt:

```
no use-optimized-talkspurt
```

use-optimized-transience

Enables or disables the use of optimized transience.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default | no ] use-optimized-transience
```

default

Returns the command to its default value of enabled.

no

Disables the use of optimized transience.

Usage

Use this command to enable or disable the use of optimized transience.

Example

The following command enables the use of optimized transience.

```
use-optimized-transience
```

The following command disables the use of optimized transience.

```
no use-optimized-transience
```

use-timer-based-compression

Enables or disables timer-based compression of the RTP time stamp (TS) at the compressor.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default | no ] use-timer-based-compression
```

default

Returns the command to its default value of enabled.

no

Disables the use of timer-based compression.

Usage

Use this command to enable or disable the use of timer-based compression.

Example

The following command enables the use of timer-based compression.

```
use-timer-based-compression
```

The following command disables the use of timer-based compression.

```
no use-timer-based-compression
```

use-uncomp-profile

Enables or disables the use of the Uncompressed Profile (0x0000) if required at the compressor.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[default | no ] useS-uncomp-profile
```

default

Returns the command to its default value of disabled.

no

Disables the use of the Uncompressed Profile.

Usage

Use this command to enable or disable the use of the Uncompressed Profile.

Example

The following command enables the use of the Uncompressed Profile.

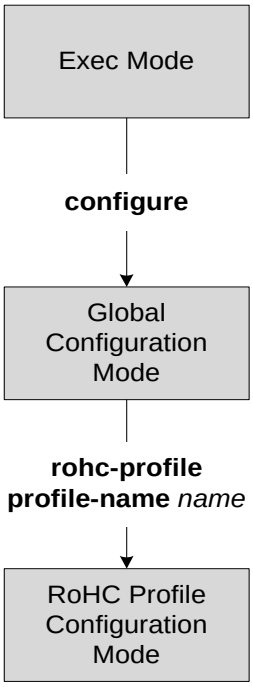
```
use-uncomp-profile
```

The following command disables the use of the Uncompressed Profile.

```
no use-uncomp-profile
```

Chapter 242
RoHC Profile Configuration Mode Commands

The RoHC Profile Configuration Mode is used to configure RoHC (Robust Header Compression) Compressor and Decompressor parameters. The profiles can then be assigned to specific subscriber sessions when RoHC header compression is configured. RoHC is not supported on GGSN.



Important: The availability of commands, keywords and variables in this mode is dependent on platform type, product version, and installed license(s).

common-options

Enters the RoHC Profile Common Options Configuration Mode where inactivity and delay timers are set to support dynamic header compression contexts and context preservation during handoffs.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default ] common-options
```

default

Reset all parameters in the RoHC Profile Common Options Configuration Mode to default values.

Usage

Use this command to enter the RoHC Profile Common Options Configuration Mode where parameters for maintaining header compression contexts and inactivity timers can be configured.
Entering this command results in the following prompt:
[*context_name*]*host*(config-rohcprofile-<*profile_name*>-common)#
RoHC Profile Common Options Configuration Mode commands are defined in the RoHC Profile Common Options Configuration Mode Commands chapter.

compression-options

Enters the RoHC Profile Compression Options Configuration Mode allowing configuration of options applied during RoHC compression for the current RoHC profile.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default ] compression-options
```

default

Reset all options in the RoHC Profile Compression Configuration Mode to their default values.

Usage

Use this command to enter RoHC Profile Compression Configuration Mode to set the compression options that are used for subscriber sessions using the current RoHC profile.
Entering this command results in the following prompt:
[*context_name*]*host*(config-rohcprofile-<*profile_name*>-comp)#
RoHC Profile Compression Options Configuration Mode commands are defined in the RoHC Profile Compression Configuration Mode Commands chapter.

Example

The following command enters RoHC Profile Compression Options Configuration Mode:

```
compression-options
```

The following command sets all compression options to their default values:

```
default compression-options
```

decompression-options

Enters the RoHC Profile Decompression Options Configuration Mode allowing configuration of options applied during RoHC decompression for the current RoHC profile.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[default ] decompression-options
```

default

Reset all options in the RoHC Profile Decompression Options Configuration Mode to their default values.

Usage

Use this command to enter RoHC Profile Decompression Options Configuration Mode to set the decompression options used for subscriber sessions using the current RoHC profile.
Entering this command results in the following prompt:
[*context_name*]*host*(config-rohcprofile-<*profile_name*>-decomp)#
RoHC Profile Decompression Options Configuration Mode commands are defined in the RoHC Profile Decompression Configuration Mode Commands chapter.

Example

The following command enters RoHC Profile Decompression Options Configuration Mode:

```
decompression-options
```

The following command sets all decompression options to their default values:

```
default decompression-options
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

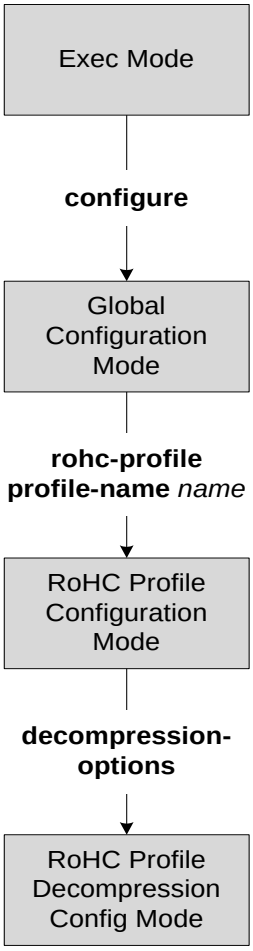
```
exit
```

Usage

Use this command to return to the parent configuration mode.

Chapter 243
RoHC Profile Decompression Configuration Mode Commands

The RoHC Profile Decompression Configuration Mode is used to configure RoHC (Robust Header Compression) Decompressor parameters.



Important: The availability of commands, keywords and variables in this mode are dependent on platform type, product version, and installed license(s).

accept-delayed-pkts

Accepts delayed packets

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default ] accept-delayed-pkts
```

default

Returns the command to its default value of disabled.

Usage

This command helps reduce packet loss during context repair.

Example

Use the following command to enable the system to accept delayed packets:

```
accept-delayed-pkts
```

context-timeout

Ensures that no expired contexts are used for data compression.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

context-timeout *seconds*

default context-timeout

default

Returns the command to its default value.

seconds

Specifies the context timeout value (in seconds) as an integer from 0 through 100.
Default: 20

Usage

The RoHC stack should periodically clean up expired contexts and release memory in case there is no data activity for the call on this context. The context cleanup period is internally calculated to be set to half of the value of the context-timeout value. This will ensure that no expired contexts are used for data compression.

Example

The following command sets the context-timeout parameter to 30 seconds:

```
context-timeout 30
```

crc-errors-fo

Sets the limits for when a NACK message is sent while in the FO (First Order) state. A NACK is sent whenever CRC errors are detected within a specified number of packets.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

crc-errors-fo-k *num_errors*

crc-errors-fo-n *num_packts*

default crc-errors-fo-k

default crc-errors-fo-n

default

Returns the command to its default value.

crc-errors-fo-k *num_errors*

Specifies the number of received packets that trigger the sending of a NACK as an integer from 1 through 10.
Default: 1

Important: *num_errors* must be less than or equal to the value specified with the **crc-errors-fo-n** command.

crc-errors-fo-n *num_packts*

Specifies the number of packets to check for CRC errors as an integer from 1 through 10.
Default: 1

Usage

Use this command to set the parameters that trigger sending a NACK message when in the FO state.

Example

To configure a NACK to be sent when 4 out of the last 10 packets have CRC errors when in the FO state, use the following commands:

```
crc-errors-fo-k 4

crc-errors-fo-n 10
```

crc-errors-so

Sets the limits for when a NACK message is sent while in the SO (Second Order) state. A NACK is sent whenever CRC errors are detected within a specified number of packets.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

crc-errors-so-k *num_errors*

crc-errors-so-n *num_packets*

default crc-errors-so-k

default crc-errors-so-n

default

Returns the command to its default value.

crc-errors-so-k *num_errors*

Specifies the number of received packets that trigger the sending of a NACK as an integer from 0 through 10.
Default: 1

Important: *num_errors* must be less than or equal to the value specified with the **crc-errors-so-n** command.

crc-errors-so-n *num_packets*

Specifies the number of packets to check for CRC errors as an integer from 1 through 10.
Default: 1

Usage

Use this command to set the parameters that trigger sending a NACK message when in the SO state.

Example

To configure a NACK to be sent when 4 out of the last 10 packets have CRC errors when in the SO state, use the following commands:

```
crc-errors-so-k 4

crc-errors-so-n 10
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

nack-limit

Sets the number of unsuccessful decompressions allowed before a NACK is sent.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

nack-limit *limit*

default nack-limit

default

Returns the command to its default value.

limit

Specifies the number of unsuccessful decompressions allowed as an integer from 0 through 20.
Default: 0

Usage

Use this command to set the maximum number of unsuccessful decompressions before a NACK message is sent.

Example

The following command sets the number of unsuccessful decompressions allowed to 10:

```
nack-limit 10
```

optimistic-mode-ack

When this command is enabled and a type 2 IR-DYN packet is successfully decompressed, an optional ACK is sent in U-mode.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default | no ] optimistic-mode-ack
```

default

Returns the command to its default value of enabled.

no

Disables the sending of the optional ACK.

Usage

Use this command to enable and disable the sending of an optional ACK in U-mode when a type 2 IR-DYN packet is successfully decompressed.

Example

To enable the sending of the optional ACK, enter the following command:

```
optimistic-mode-ack
```

To disable the sending of the optional ACK, enter the following command:

```
no optimistic-mode-ack
```

optimistic-mode-ack-limit

Sets the number of packets for which to send ACKs.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

optimistic-mode-ack-limit *num_pkts*

default optimistic-mode-ack-limit

default

Returns the command to its default value.

num_pkts

Specifies the number of packets for which to send ACKs as an integer from 0 through 20.
Default: 3

Usage

Use this command to set the number of packets to send the optional ACK for when a type 2 IR-DYN packet is successfully decompressed.

Example

Enter the following command to set the number of packets to send and ACK for to 6:

```
optimistic-mode-ack-limit 6
```

Use the following command to set the number of packets to send an ACK for back to the default of 3:

```
default optimistic-mode-ack-limit
```

piggyback-wait-time

Specifies the time in milliseconds to wait for a feedback packet to be picked up as piggybacked feedback by the associated compressor.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

piggyback-wait-time *m_secs*

default piggyback-wait-time

default

Returns the command to its default value.

m_secs

Specifies the time (in milliseconds) to wait for a feedback packet to be picked up as an integer value from 0 through 1000.
Default: 80

Usage

Use this command to set the time in milliseconds to wait for a feedback packet to be picked up as piggybacked feedback by the associated compressor.

Example

The following command sets the wait time to 120 ms:

```
piggyback-wait-time 120
```

preferred-feedback-mode

Specifies the preferred feedback mode to use between the compressor and the decompressor

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
preferred-feedback-mode { bidirectional-optimistic | bidirectional-reliable |
unidirectional }

default preferred-feedback-mode
```

default

Returns the command to its default setting of bidirectional-optimistic.

bidirectional-optimistic

This mode is similar to the Unidirectional mode, with the exception of a feedback channel used to send error recovery requests from the decompressor to compressor.
This is the default mode.

bidirectional-reliable

Reliable mode makes extensive use of a feedback channel to avoid packet loss from context invalidation. A secure reference model is used instead of the optimistic approach used in the other modes. With the secure reference model, the confidence of the compressor depends on acknowledgements from the decompressor for every context updating packet.
Periodically the compressor sends context updating packets repeatedly until an acknowledgement is received from the decompressor.

unidirectional

Packets are sent in only one direction, from the compressor to the decompressor.

Usage

Use this command to specify the preferred feedback method to use between the compressor and the decompressor for the current RoHC profile.

Example

Use the following command to set the preferred feedback mode to bidirectional-reliable:

```
preferred-feedback-mode bidirectional-reliable
```

rtp-sn-p

Specifies the value of p in RTP SN (RTP Sequence Number) calculation. Least Significant Bits (LSB) encoding is used for header fields whose values are usually subject to small changes. With LSB encoding, the k least significant bits of the field value are transmitted instead of the original field value, where k is a positive integer. After receiving k bits, the decompressor derives the original value using a previously received value as reference (v_ref). The scheme is guaranteed to be correct if the compressor and the decompressor each use interpretation intervals as follows:

- In which the original value resides
- And in which the original value is the only value that has the exact same k least significant bits as those transmitted.

The interpretation interval can be described as a function:

f(v_ref, k). Let f(v_ref, k) = [v_ref - p, v_ref + (2^k - 1) - p]

Where p is an integer.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

rtp-sn-p *value*

default rtp-sn-p

default

Returns the command to its default value.

value

Specifies the number the value of p in the RTP SN calculation as an integer from 0 through 999.

Usage

Use this command to set the value to use for p when performing the RTP SN calculation.

Example

The following command sets the RTP Sequence Number integer “p” value to 100:

```
rtp-sn-p 100
```

rtp-sn-p-override

Allows an override of p in RTP SN calculation. This is disabled by default.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default | no ] rtp-sn-p-override
```

default

Returns the command to its default value of disabled.

no

Disables overriding p in RTP SN calculation.

Usage

Use this command to allow an override of p in RTP SN calculations.

Example

The following command enables the override of p in the RTP SN calculation:

```
rtp-sn-p-override
```

sliding-window-ts

Computes jitter as described in RFC 3095,[4.5.4]

Product

HSGW, PDSN

Privilege

Administrator

Syntax

sliding-window-ts *size*

default sliding-window-ts

default

Returns the command to its default value of 4.

size

Sets the size of the sliding window. *size* must be an integer from 1 through 1000.
Default: 4

Usage

Use this command to set the size of the sliding window used to compute jitter for the current RoHC profile.

Example

The following command sets the sliding window size to 500:

```
sliding-window-ts 500
```

use-clock-option

Controls usage of the RoHC clock option. The clock option informs the compressor of the clock resolution of the decompressor. This allows the compressor to estimate the jitter introduced by the clock of the decompressor when doing timer-based compression of the RTP timestamp.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default | no ] use-clock-option
```

default

Returns the command to its default value of enabled.

no

Disables use of the RoHC clock option.

Usage

Use this command to enable and disable the use of the RoHC clock option.

Example

The following command enables RoHC clock option usage:

```
use-clock-option
```

The following command disables RoHC clock option usage:

```
no use-clock-option
```

use-crc-option

Controls usage of the RoHC cyclic redundancy check (CRC) option. The CRC option contains an 8-bit CRC computed over the entire feedback payload, without the packet type and code octet, but including any CID fields,

Product

HSGW, PDSN

Product

Administrator

Syntax

```
[ default | no ] use-crc-option
```

default

Returns the command to its default value of enabled.

no

Disables use of the CRC option.

Usage

Use this command to enable and disable the use of the RoHC CRC option.

Example

The following command enables RoHC CRC option usage:

```
use-crc-option
```

The following command disables RoHC CRC option usage:

```
no use-crc-option
```

use-feedback

Controls use of the feedback channel. A feedback channel sends error recovery requests and (optionally) acknowledgments of significant context updates from the decompressor to the compressor.

Product

HSGW, PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] use-feedback
```

default

Returns the command to its default value of disabled.

no

Disables use of the feedback channel.

Usage

Use this command to enable and disable the use of the RoHC feedback channel.

Example

The following command enables RoHC feedback channel usage:

```
use-feedback
```

The following command disables RoHC feedback channel usage:

```
no use-feedback
```

use-jitter-option

Controls usage of RoHC jitter option. The jitter option allows the decompressor to report the maximum jitter it has observed

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default | no ] use-jitter-option
```

default

Returns the command to its default value of enabled.

no

Disables use of the jitter option.

Usage

Use this command to enable and disable the use of the RoHC jitter option.

Example

The following command enables RoHC jitter option usage:

```
use-jitter-option
```

The following command disables RoHC jitter option usage:

```
no use-jitter-option
```

use-reject-option

Controls usage of RoHC reject option. The reject option informs the compressor that the decompressor does not have sufficient resources to handle the flow.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default | no ] use-reject-option
```

default

Returns the command to its default value of disabled.

no

Disables use of the reject option.

Usage

Use this command to enable and disable the use of the RoHC reject option.

Example

The following command enables RoHC reject option usage:

```
use-reject-option
```

The following command disables RoHC reject option usage:

```
no use-reject-option
```

use-sn-not-valid-option

Controls usage of the RoHC SN not valid option. The sn-not-valid option indicates that the SN of the feedback is not valid. A compressor must not use the SN of the feedback to find the corresponding sent header when this option is present.

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default | no ] use-sn-not-valid-option
```

default

Returns the command to its default value of enabled.

no

Disables use of the sn-not-valid option.

Usage

Use this command to enable and disable the use of the RoHC sn not valid option.

Example

The following command enables RoHC sn not valid option usage:

```
use-sn-not-valid-option
```

The following command disables RoHC sn not valid option usage:

```
no use-sn-not-valid-option
```

use-sn-option

Controls usage of RoHC sn option. The sn option provides eight additional bits of SN (Sequence Number, usually the RTP Sequence Number.)

Product

HSGW, PDSN

Privilege

Administrator

Syntax

```
[ default | no ] use-sn-option
```

default

Returns the command to its default value of enabled.

no

Disables use of the SN option.

Usage

Use this command to enable and disable the use of the RoHC SN option.

Example

The following command enables RoHC SN option usage:

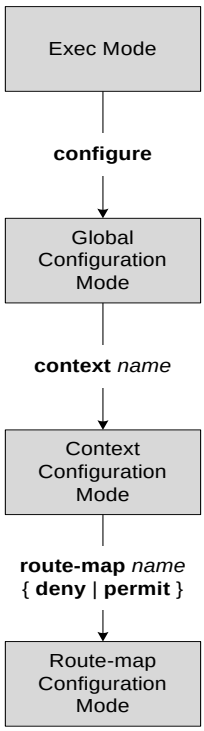
```
use-sn-option
```

The following command disables RoHC SN option usage:

```
no use-sn-option
```

Chapter 244
Route-map Configuration Mode Commands

The Route-Map Configuration sub-mode is used for the OSPFv2 and BGP-4 routing protocols. This mode includes commands that configure matching rules and set actions to perform on matched routes.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

match as-path

Matches an Autonomous System (AS) path access list

Product

HA

Privilege

Security Administrator, Administrator

Syntax

[no] match as-path *AS_list*

no

Disables matching the specified AS path access list.

AS_list

Specifies the name of an AS path access list for matching as an alphanumeric string of 1 through 79 characters.

Usage

This command is used for BGP-4 routing to specify an AS path access list to be matched. Refer to the **ip as-path access-list** command for more information.

Example

To match entries in an AS path access list named *ASlist1*, enter the following command;

```
match as-path ASlist1
```

match interface

Specifies the next-hop interface name of a route to be matched.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] match interface *interface-name*

no

Disables matching the specified interface name.

interface-name

Specifies the name of the virtual interface for matching as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to specify the next hop interface name for routes to be matched.

Example

To match routes that have the next hop interface specified as *Interface123*, enter the following command:

```
match interface Interface123
```

To disable matching routes that have the next hop interface specified as *Interface123*, enter the following command:

```
no match interface Interface123
```

match ip address

Matches routes with entries in a route-access-list or prefix-list.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] match ip address { prefix-list | route-access-list } *list_name*

no

Disables matching from the specified prefix list or route access list.

prefix-list

Matches any routes with entries in a prefix-list.

route-access-list

Matches any routes with entries in a route-access-list

list_name

Specifies the name of the IP prefix list or IP route access-list as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to match routes specified in a route-access-list or prefix-list.

Example

To match routes that are specified in a prefix list named *Prefix100*, enter the following command:

```
match ip address prefix-list Prefix100
```

To disable matching routes that are specified in a prefix list named *Prefix100*, enter the following command:

```
no match ip address prefix-list Prefix100
```

match ip next-hop

Matches next-hop IP addresses with entries in specified standard prefix-list or route-access-list.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] match ip address next-hop { prefix-list | route-access-list }*list_name*

prefix-list

Matches any routes that have a next-hop router address that has an entry in the specified prefix list.

route-access-list

Matches any routes that have a next-hop router address that has an entry in the specified route-access-list.

list_name

Specifies the name of the IP prefix-list or IP route-access-list as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to match next-hop IP addresses that have entries in the specified prefix-list or route-access-list.

Example

To match next-hop addresses with entries in a prefix-list named *Prefix100*, enter the following command:

```
match ip address next-hop prefix-list Prefix100
```

To disable matching next-hop addresses with entries in a prefix-list named *Prefix100*, enter the following command:

```
no match ip address next-hop prefix-list Prefix100
```

match metric

Matches routes that have the specified route metric.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] match metric *metric_value*

no

Disables matching of the specified route metric.

metric_value

Specifies the route metric to match as an integer from 0 through 4294967295.

Usage

Use this command to match routes that have the specified route metric.

Example

To match routes with the route metric of *1200*, enter the following command:

```
match metric 1200
```

To disable matching routes with a route metric of *1200*, enter the following command:

```
no match metric 1200
```

match origin

Matches the origin code learned from BGP. This command is for route maps that are used with BGP routing only.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] match origin { egp | igp | incomplete }
```

no

Disables matching of the origin code.

egp

Matches origins learned via the External Gateway Protocol (EGP)

igp

Match origins learned via the local Interior Glittery Protocol (IGP)

incomplete

Match origins with unknown heritage.

Usage

Use this command to match origin codes for BGP routing.

Example

To match origin codes learned from EGP, enter the following command:

```
match origin egp
```

match route-type external

Match external Open Shortest Path First (OSPF) routes of the specified type.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] match route-type external { type-1 | type-2 }
```

type-1

Only matches type-1 external routes.

type-2

Only matches type-2 external routes.

Usage

Use this command to match external routes of a specific type.

Example

The following command matches all external routes that are type-2:

```
match route-type external type-2
```

The following command disables matching external routes that are type-2:

```
no match route-type external type-2
```

match tag

Matches routes with the specified route tag value.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] match tag *tag_value*

no

Disables matching routes with the specified route tag value.

tag_value

Specifies the route tag value to match as an integer from 0 through 4294967295.

Usage

Use this command to match routes that have the specified route tag value.

Example

Use the following command match routes that have a route tag value of *1234*:

```
match tag 1234
```

Use the following command to disable matching routes that have a route tag value of *1234*:

```
no match tag 1234
```

set as-path

Modifies an Autonomous System (AS) path for a route by adding the specified AS numbers to the front of the path.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

[no] set as-path prepend *ASN*

no

Disables prepending the AS path. Any previously set prepends are removed.

prepend

Prepends the AS path.

ASN

AS number(s) to be prepended to the AS path. You can specify up to 16 different AS numbers to be prepended in the order specified. Each AS number must be separated by a space. *ASN* must be an integer from 1 through 65535.

Usage

Use this command to add up to 16 specified AS numbers to the front of the AS path.

Example

The following command prepends the AS numbers *100*, *200*, and *1000* to matching AS paths:

```
set as-path prepend 100 200 1000
```

set ip next-hop

Sets the IP address that is applied as the next hop for routes.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] set ip next-hop *ip_address*

no

Disables the specified next hop address.

ip_address

Specifies the IP address of the next hop to which packets are output, entered using IPv4 dotted-decimal notation.

Usage

Use this command to set the IP address that is used as the next hop for routes.

Example

To set the next hop for routes to the IP address *192.168.2.100*, use the following command:

```
set ip next-hop 192.168.2.100
```

To disable setting the next hop for routes to the IP address *192.168.2.100*, use the following command:

```
no set ip next-hop 192.168.2.100
```

set metric

Sets the route metric for matching routes to a specified value.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] set metric *metric_value*

metric_value

Specifies the metric value that is set for routes as an integer from 1 through 16777214.

Usage

Use this command to set the route metric for matched routes.

Example

To set the route metric to *12345*, use the following command;

```
set metric 12345
```

To disable setting the route metric to *12345*, enter the following command;

```
no set metric 12345
```

set metric-type

This command sets the route metric type to either Type-1 or Type-2 in the AS-external-LSA.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] set metric-type { type-1 | type-2 }
```

type-1

Sets the route metric to external type-1.

type-2

Sets the route metric to external type-2

Usage

Use this command to set the route metric to either external type-1 or external type-2.

Example

To set the route metric to type-1, enter the following command:

```
set metric type-1
```

To disable setting the metric to type, enter the following command:

```
no set metric type-1
```

set origin

Sets the Border Gateway Protocol (BGP) origin code to a specified value. This command is for route maps that are used with BGP routing only.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] set origin { egp | igp | incomplete }
```

no

Disables setting the origin code.

egp

Sets the origin code to specify that the path is from a remote External Gateway Protocol (EGP) system.

igp

Sets the origin code to specify that the path is from a local Interior Gateway Protocol (IGP) system.

incomplete

Sets the origin code to specify that the path is from an unknown system.

Usage

Use this command to set a specified origin code for BGP.

Example

To set the origin code to be from an External Gateway Protocol (EGP) system, enter the following command:

```
set origin egp
```

set tag

Sets the route tag value for matched routes.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] set tag *tag_value*

no

Disable setting the route tag to the specified value.

tag_value

Specifies the route tag value as an integer from 0 through 4294967295.

Usage

Use this command to set the route tag value that is applied to all matched routes.

Example

To set the route tag value to *12345*, enter the following command:

```
set tag 12345
```

To disable setting the route tag value to *12345*, enter the following command:

```
no set tag 12345
```

set weight

Sets the weight in the routing table for matching routes to the specified value.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] set weight value
```

no

Disable setting the routing weight value.

value

Specifies the weight in the routing table as an integer from 1 through 4294967295.

Usage

Use this command to set the routing table weight on matched routes.

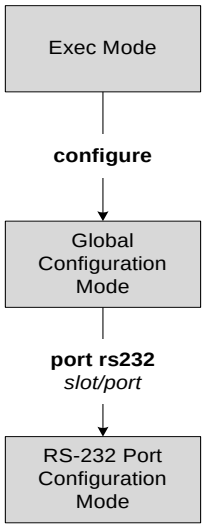
Example

The following command sets the routing table weight for matched routes to *1000*:

```
set weight 1000
```

Chapter 245
RS-232 Port Configuration Mode Commands

The RS-232 Port Configuration Mode is used to manage the RS-232 ports on the SPIO cards.



default

Restores the port's default speed and communication mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
default { preferred slot | terminal { all | databits | flowcontrol | parity | speed |
stopbits }
```

preferred slot

Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a **port switch to** command to return service to the original port.

terminal { all | databits | flowcontrol | parity | speed | stopbits }

Sets the terminal settings for the RS-232 port to their default settings.
all: Restores all settings to their default values.
databits: Restores the databits setting to its default value of 8.
flowcontrol: Restores the flowcontrol setting to its default value of none.
parity: Restores the parity setting to its default value of none.
speed: Restores the speed setting to its default value of 9600.
stopbits: Restores the stopbits setting to its default value of 1.

Usage

Restores port-level parameters to their default values.

Example

The following command restores all terminal settings to their default values:

```
default terminal all
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

preferred slot

Assigns revertive or non-revertive control to port redundancy auto-recovery.

Default: non-revertive operation

Product

PDSN, FA, HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

preferred slot *slot#*

no preferred slot *slot#*

no

Disables revertive, or auto-recovery, operation for selected port.

slot#

Identifies the physical chassis slot where the SPIO card is installed.

Usage

This command enables or disables revertive port redundancy, wherein after a port failover, when the original port is restored to service (such as link up) the system will return service to that port automatically.
Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a port switch to command to return service to the original port.
This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual line cards or SPIO cards. For example, ports 1 through 4 could be configured as "preferred" on the line card in slot 17, while ports 5 through 8 are "preferred" on the line card in slot 33. In this scenario, both line cards would be in an Active operational state while still providing LC and port redundancy for the other.

Important: This command is not supported on all platforms.

Example

```
preferred slot 24
```

snmp trap link-status

Enables or disables the generation of an SNMP trap for link status changes.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
snmp trap link-status

no snmp trap link-status
```

no

Disables the sending of traps for link status changes.

Usage

Enable link status change traps when a monitoring facility can use the information or if there are trouble shooting activities are in progress.

Example

```
snmp trap link-status

no snmp trap link-status
```

terminal

Configures the console port on the SPIO.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
terminal { carrierdetect { off | on } | databits { 7 | 8 } | flowcontrol { hardware |
none } | parity { even | none | odd } | speed { 115200 | 19200 | 38400 | 57600 | 9600 } |
stopbits { 1 | 2 } }
```

carrierdetect { off | on }

Default:
Specifies whether or not the console port is to use carrier detect when connecting to a terminal.

databits { 7 | 8 }

Default: 8
Specifies the number of data bits used to transmit and receive characters.

flowcontrol { hardware | none }

Default: none
Specifies how the flow of data is controlled between the SPIO and a terminal.

parity { even | none | odd }

Default: none
Specifies the type of error checking used on the port.
even: Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits even.
none: Disables error checking.
odd: Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits odd.

speed { 115200 | 19200 | 38400 | 57600 | 9600 }

Default: 9600
Specifies the flow of data in bits per second between the console port and terminal.

stopbits { 1 | 2 }

Default: 1
Specifies the number of stop bits between each transmitted character.

Usage

Sets the SPIO console port parameters for communication with the terminal device.

Example

The following command sets the SPIO's console port. The terminal must support these values.

```
terminal carrierdetect off databits 7 flowcontrol hardware parity even
speed 115200 stopbits 1
```

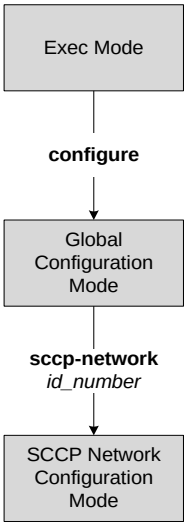
Chapter 246
SCCP Network Configuration Mode Commands

The SCCP Network Configuration Mode is used to configure properties for Signaling Connection Control Part (SCCP) services for SS7.

In this mode, the command prompt should be similar to:

```
[local]hostname(config-sccp-network-<sccp_id>)#
```

Signaling Connection Control Part (SCCP) is a routing protocol in the SS7 protocol suite in layer 4, which provides end-to-end routing for TCAP messages to their proper database.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

associate

Associates an SS7 routing domain with the SCCP network.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

associate ss7-routing-domain *rd_id*

no associate

no

Removes the association with the SS7 routing domain from the system configuration.

rd_id

This number identifies an already defined SS7 routing domain.
rd_id: enter an integer from 1 through 12.

Usage

Use this command to associate SS7 routing domain configurations with SCCP network configurations.

Example

The following command associates the SCCP network with SS7 routing domain 2:

associate ss7-routing-domain *2*

description

This command defines a string that describes the SCCP network. The description is used for operator reference.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

description *string*

no description

string

This is a string to describe the SCCP network.
string must be an alphanumeric string from 1 through 127 characters in length. If there are spaces in the string the string must be enclosed in double-quotes. For example; “This is a Description”.

no

Removes the description from the system configuration.

Usage

Use this command to configure a description of this SCCP service for operator reference.

Example

The following command sets the description to “This is the SCCP Service Number 1”:

```
description ”This is the SCCP Service Number 1.”
```

destination

This command configures the SCCP network destination information. Use this command multiple times to set all of the destination information required.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

destination dpc *pt_code* **{ name** *route_name* **| next-hop** *pt_code* **[priority** *priority* **] | ssn** *subsys_num* **| version** *sccp_ver* **}**

no destination dpc *p_code* **[name** *route_name* **| ssn** *ssn_num* **| version** *sccp_ver* **]**

no

Deletes the specified destination information from the SCCP network configuration.

dpc *pt_code*

Specifies the SCCP destination point code.
pt_code: Must be in SS7 point code dotted-decimal ###.###.### format or decimal ######## format.

name *route_name*

The name of the SCCP destination route.
route_name: enter an alphanumeric string from 1 through 64 characters in length.

next-hop *pt_code* **[priority** *priority*

Associates the next destination defined in the SS7 routing domain and assigns the next-hop a priority for use.
pt_code: Must be in SS7 point code dotted-decimal ###.###.### format or decimal ######## format.
priority: Must be an integer from 0 to 15, with 0 setting the highest priority.

ssn *subsys_num*

The destination subsystem number.
subsys_num: enter an integer from 1 through 255.

version *sccp_ver*

sccp_ver: enter one of the following to select the SCCP variant:

- ANSI88
- ANSI92
- ANSI96
- BELL05
- CHINA
- GSM0806
- ITU88

- ITU92
- ITU96

Usage

Use this command to configure the destination information for the SCCP network.

Example

The following commands set the name of the destination route to default_route, the subsystem number to 1, and the variant version to ITU96, all with a destination point code of 1:

```
destination dpc 1 name default_routedestination dpc 1 ssn 1destination
dpc version ITU96
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

SGSN , HNB-GW

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Return to the Exec mode.

exit

Exits the current configuration mode and returns to the global configuration mode.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Return to the global configuration mode.

global-title-translation

This command associates a GTT address-map with this SCCP network.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

global-title-translation address-map instance *instance*

no global-title-translation address-map instance *instance*

no

Deletes the GTT address-map instance associated with this SCCP network.

instance

This value uniquely identifies a specific previously defined instance of a GTT address-map.
instance: enter an integer from 1 to 4096.

Usage

Use this command to link a GTT address-map, configured with the GTT Address Map configuration mode, to a specific SCCP network configuration.

Example

global-title-translation address-map instance *gtt-map1*

hop-count

This command specifies the hop count for this SCCP network.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

hop-count *hop_cnt*

default hop-count

default

Resets the hop-count value to the system default of 5.

hop_cnt

The hop count to assign to this SCCP network.
hop_cnt: enter an integer from 1 to 15.

Usage

Use this command to define the hop count for this SCCP network.

Example

The following command sets the hop count to 3:

hop-count *3*

self-point-code

This command specifies the SS7 point code for this SCCP service.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

self-point-code *point_code*

no self-point-code

no

Deletes the configured self point code.

point_code

Defines the point code to assign to this SCCP network service.
point_code: value entered must adhere to the point code variant selected when the SCCP network instance was defined:

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- a string of 1 to 11 combined digits ad period.

Usage

Use this command to assign the self point code to use for this SCCP service.

Example

The following command sets an ITU-based point code for this SCCP service:

self-pointcode *4.121.5*

The following command removes the configured self-point code:

no self-pointcode

timeout

This command configures the timeout parameters for this SCCP network.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

```
timeout { attack-timer | congestion-timer | conn-est-timer | crd-timer | decay-timer |
iar-timer | ias-timer | interval-timer | reassembly-timer | release-timer | repeat-
release-timer | reset-timer | sst-timer } +

default timeout

no timeout timer
```

attack-timer *time*

Defines the time before the attack timer expires.
time: enter an integer between 1 and 10.

congestion-timer *time*

Defines the time before the congestion timer expires.
time: enter an integer between 1 and 10.

conn-est-timer *time*

Defines the time before the connection timer expires.
time: enter an integer between 6 and 12.

crd-timer *time*

Defines the time before the coordinated-state-change timer expires.
time: enter an integer between 60 and 120.

decay-timer *time*

Defines the time before the decay timer expires.
time: enter an integer between 1 and 10.

iar-timer *time*

Defines the time before the inactivity-receive timer expires.
time: enter an integer between 60 and 120.

ias-timer *time*

Defines the time before the inactivity-send timer expires.
time: enter an integer between 30 and 60.

interval-timer *time*

Defines the time before the interval timer expires.
time: enter an integer between 6 and 12

reassembly-timer *time*

Defines the time before the reassembly-timer expires.
time: enter an integer between 10 and 20.

release-timer *time*

Defines the time before the release-assembly timer expires.
time: enter an integer between 1 and 2.

repeat-release-timer *time*

Defines the time before repeat-release timer expires.
time: enter an integer between 1 and 2

reset-timer *time*

Defines the amount of time before the reset timer expires.
time: enter an integer between 1 and 2

sst-timer *time*

Defines the amount of time before the subsystem status test timer expires.
time: enter an integer between 5 and 1200.

default

Resets the timeout parameter to the system default.

no

Deletes the specified timer configuration.

Usage

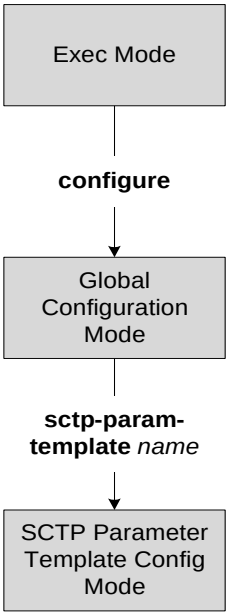
Use this command to assign timeout timers and timeout values for this SCCP service.

Example

timeout reset-timer *75*

Chapter 247
SCTP Parameter Template Configuration Mode Commands

This chapter provides information about commands used to configure parameters for Stream Control Transmission Protocol (SCTP) associations. The commands become part of a template that can be associated with services running on the system.



sctp-alpha

Configures the SCTP retransmission timeout (RTO) alpha value.

Product

MME

Privilege

Administrator

Syntax

sctp-alpha *value*

default sctp-alpha

default

Returns the command to its default setting of 5.

value

Default: 5
Specifies the SCTP retransmission timeout alpha value. *value* must be an integer from 0 through 65535.

Usage

Use this command to configure the SCTP RTO alpha value. The RTO alpha value is used in calculating the smoothed round-trip time (SRTT) and the round-trip time variation (RTTVAR) for new round trip time (RTT) measurements.

Example

The following command sets the SCTP RTO alpha value to *10*:

```
sctp-alpha 10
```

sctp-alt-accept-flag

Configures the SCTP alternate accept flag for additional life time for the association.

Product

MME

Privilege

Administrator

Syntax

```
sctp-alt-accept-flag { disable | enable }

default sctp-alt-accept-flag
```

default

Returns the command to its default setting of enable.

disable | enable

Specifies if the alternate accept flag is enabled or disabled.

Usage

Use this command to configure the SCTP alternate accept flag for additional life time for the association.

Example

The following command disables the alternate accept flag for the SCTP association:

```
sctp-alt-accept-flag disable
```

sctp-beta

Configures the SCTP retransmission timeout (RTO) beta value.

Product

MME

Privilege

Administrator

Syntax

sctp-beta *value*

default sctp-beta

default

Returns the command to its default setting of 10.

value

Specifies the SCTP retransmission timeout beta value as an integer from 0 through 65535. Default: 10

Usage

Use this command to configure the SCTP RTO beta value. The RTO beta value is used in calculating the smoothed round-trip time (SRTT) and the round-trip time variation (RTTVAR) for new round trip time (RTT) measurements.

Example

The following command sets the SCTP RTO beta value to *20*:

```
sctp-beta 20
```

sctp-checksum-type

Configures the checksum type used to increase the integrity of the SCTP packets during transmission.

Product

MME

Privilege

Administrator

Syntax

```
sctp-checksum-type { adler32 | crc32 }

default sctp-checksum-type
```

default

Returns the command to its default setting of CRC32.

adler32 | crc32

Specifies the type of checksum used to increase data integrity of SCTP packets.
adler32: Specifies that the Adler-32 checksum algorithm is used to increase data integrity for SCTP packets.
crc32: Specifies that a 32-bit cyclic redundancy check is used to increase data integrity of SCTP packets.

Usage

Use this command to select the checksum for data integrity of SCTP packets.

Example

The following command enables the Adler-32 checksum algorithm used to increase data integrity of SCTP packets:

```
sctp-checksum-type adler32
```

sctp-cookie-life

Configures the lifetime of the SCTP cookie.

Product

MME

Privilege

Administrator

Syntax

sctp-cookie-life *value*

default sctp-cookie-life

default

Returns the command to its default setting of 600 (60000 milliseconds).

value

Default: 600 (60000 milliseconds)
Specifies the lifetime of the SCTP cookie. *value* is an integer from 50 through 1200. The range translates to 5000 milliseconds to 120000 milliseconds, as the granularity is in 100-millisecond increments.

Usage

Use this command to configure the lifetime of the SCTP cookie.

Example

The following command configures the lifetime of the SCTP cookie to 80000 milliseconds:

```
sctp-cookie-life 800
```

sctp-max-assoc-retx

Configures the maximum number of retransmissions for SCTP associations.

Product

MME

Privilege

Administrator

Syntax

sctp-max-assoc-retx *value*

default sctp-max-assoc-retx

default

Returns the command to its default setting of 10.

value

Specifies the maximum number of retransmissions allowed by this template for SCTP associations as an integer from 0 through 255. Default: 10

Usage

Use this command to configure the maximum number of retransmissions allowed by this template for SCTP associations.

Example

The following command configures the maximum number of retransmissions to 7:

```
sctp-max-assoc-retx 7
```

sctp-max-in-strms

Configures the maximum number of incoming SCTP streams allowed by the template.

Product

MME

Privilege

Administrator

Syntax

sctp-max-in-strms *value*

default sctp-max-in-strms

default

Returns the command to its default setting of 16.

value

Specifies the maximum number of incoming SCTP streams allowed by the template as an integer from1 through 16. Default: 16

Usage

Use this command to configure the maximum number of incoming SCTP streams allowed by the template.

Example

The following command configures the maximum number of incoming SCTP streams allowed by the template to *5*:

```
sctp-max-in-strms 5
```

sctp-max-init-retx

Configures the maximum number of retransmissions of SCTP initiations allowed by the template.

Product

MME

Privilege

Administrator

Syntax

sctp-max-init-retx *value*

default sctp-max-init-retx

default

Returns the command to its default setting of 5.

value

Specifies the maximum number of retransmissions of SCTP initiations allowed by the template as an integer from 0 through 255. Default: 5

Usage

Use this command to configure the maximum number of retransmissions of SCTP initiations allowed by the template.

Example

The following command configures the maximum number of retransmissions of SCTP initiations allowed by the template to *10*:

```
sctp-max-init-retx 10
```

sctp-max-mtu-size

Configures the maximum transmission unit (MTU) size (in bytes) for SCTP streams allowed by the template.

Product

MME

Privilege

Administrator

Syntax

sctp-max-mtu-size *bytes*

default sctp-max-mtu-size

default

Returns the command to its default setting of 1500 bytes.

bytes

Specifies the maximum MTU size (in bytes) for SCTP streams allowed by the template as an integer from 508 through 65535. Default: 1500

Usage

Use this command to configure the maximum MTU size, in bytes, for SCTP streams allowed by the template.

Example

The following command configures the maximum MTU size for SCTP streams allowed by the template to *3000*:

```
sctp-max-mtu-size 3000
```

sctp-max-out-strms

Configures the maximum number of outgoing SCTP streams allowed by the template.

Product

MME

Privilege

Administrator

Syntax

sctp-max-out-strms *value*

default sctp-max-out-strms

default

Returns the command to its default setting of 16.

value

Specifies the maximum number of outgoing SCTP streams allowed by the template as an integer from 1 through 16. Default: 16

Usage

Use this command to configure the maximum number of outgoing SCTP streams allowed by the template.

Example

The following command configures the maximum number of outgoing SCTP streams allowed by the template to *5*:

```
sctp-max-out-strms 5
```

sctp-max-path-retx

Configures the maximum number of retransmissions of SCTP paths allowed by the template.

Product

MME

Privilege

Administrator

Syntax

sctp-max-path-retx *value*

default sctp-max-path-retx

default

Returns the command to its default setting of 5.

value

Specifies the maximum number of retransmissions of SCTP paths allowed by the template as an integer from 0 through 255. Default: 5

Usage

Use this command to configure the maximum number of retransmissions of SCTP paths allowed by the template. An SCTP path is a connection between an endpoint address and a peer endpoint address.

Example

The following command configures the maximum number of retransmissions of SCTP paths allowed by the template to *10*:

```
sctp-max-path-retx 10
```

sctp-min-mtu-size

Configures the minimum maximum transmission unit (MTU) size (in bytes) for SCTP streams allowed by the template.

Product

MME

Privilege

Administrator

Syntax

sctp-min-mtu-size *bytes*

default sctp-min-mtu-size

default

Returns the command to its default setting of 508 bytes.

bytes

Specifies the minimum MTU size (in bytes) for SCTP streams allowed by the template as an integer from 508 through 65535. Default: 508

Usage

Use this command to configure the minimum MTU size, in bytes, for SCTP streams allowed by the template.

Example

The following command configures the minimum MTU size for SCTP streams allowed by the template to *1000*:

```
sctp-min-mtu-size 1000
```

sctp-rto-initial

Configures the initial time for SCTP retransmission timeouts (RTOs) allowed by the template.

Product

MME

Privilege

Administrator

Syntax

sctp-rto-initial *value*

default sctp-rto-initial

default

Returns the command to its default setting of 30 (3000 milliseconds).

value

Specifies the initial time for SCTP RTO as an integer from 1 through 1200. The granularity is in 100ms increments (20 = 2000ms). Default: 30 (3000 milliseconds)

Usage

Use this command to configure the initial time for SCTP RTOs allowed by the template.

Example

The following command configures the initial SCTP RTO to 6000ms:

```
sctp-rto-initial 60
```

sctp-rto-max

Configures the maximum time for SCTP retransmission timeouts (RTOs) allowed by the template.

Product

MME

Privilege

Administrator

Syntax

sctp-rto-max *value*

default sctp-rto-max

default

Returns the command to its default setting of 600 (60000 milliseconds).

value

Specifies the maximum time for SCTP RTOs allowed by the template as an integer from 50 through 1200. The granularity is in 100ms increments (120 = 12000ms). Default: 600 (60000 milliseconds)

Usage

Use this command to configure the maximum time for SCTP RTOs allowed by the template.

Example

The following command configures the maximum time for SCTP RTOs allowed by the template to 120000ms:

```
sctp-rto-max 120
```

sctp-rto-min

Configures the minimum time for SCTP retransmission timeouts (RTOs) allowed by the template.

Product

MME

Privilege

Administrator

Syntax

sctp-rto-min *value*

default sctp-rto-min

default

Returns the command to its default setting of 10 (1000 milliseconds).

value

Specifies the minimum time for SCTP RTOs allowed by the template as an integer from 1 through 500. The granularity is in 100ms increments (20 = 2000ms). Default: 10 (1000 milliseconds)

Usage

Use this command to configure the minimum time for SCTP RTOs allowed by the template.

Example

The following command configures the minimum time for SCTP RTOs allowed by the template to 2000ms:

```
sctp-rto-min 20
```

sctp-sack-frequency

Configures the frequency of SCTP selective acknowledgements allowed by the template.

Product

MME

Privilege

Administrator

Syntax

sctp-sack-frequency *value*

default sctp-sack-frequency

default

Returns the command to its default setting of 2.

value

Specifies the frequency of SCTP selective acknowledgements allowed by the template as an integer from 1 through 20. Default: 2

Usage

Use this command to configure the frequency of SCTP selective acknowledgements allowed by the template.

Example

The following command configures the frequency of SCTP selective acknowledgements allowed by the template to 10:

```
sctp-sack-frequency 10
```

sctp-sack-period

Configures the period for SCTP selective acknowledgements allowed by the template.

Product

MME

Privilege

Administrator

Syntax

sctp-sack-period { *value* | units-10ms *value* }

default sctp-sack-period

default

Returns the command to its default setting of 2 (200 milliseconds).

value

Specifies the period for SCTP selective acknowledgements allowed by the template as an integer from 0 through 5. The granularity is in 100ms increments (3 = 300ms). Default: 2 (200 milliseconds)

units-10ms *value*

Specifies that the integer added as *value* is to be calculated using 10ms granularity for this command. *value* is an integer from 0 through 50.

Usage

Use this command to configure the period for SCTP selective acknowledgements allowed by the template.

Example

The following command configures the period for SCTP selective acknowledgements allowed by the template to 400ms (using the 10ms granularity):

```
sctp-sack-period units-10ms 40
```

sctp-start-mtu-size

Configures the start maximum transmission unit (MTU) size (in bytes) for SCTP streams allowed by the template.

Product

MME

Privilege

Administrator

Syntax

sctp-start-mtu-size *bytes*

default sctp-start-mtu-size

default

Returns the command to its default setting of 1500 bytes.

bytes

Specifies the start MTU size (in bytes) for SCTP streams allowed by the template as an integer from 508 through 65535. Default: 1500

Usage

Use this command to configure the start MTU size, in bytes, for SCTP streams allowed by the template.

Example

The following command configures the start MTU size for SCTP streams allowed by the template to *3000*:

```
sctp-start-mtu-size 3000
```

timeout

Configures timeouts for SCTP data chunk bundle transmissions and/or SCTP heartbeat request responses.

Product

MME

Privilege

Administrator

Syntax

timeout { sctp-bundle *value* **| sctp-heart-beat** *value* **}**

[default | no] timeout { sctp-bundle | sctp-heart-beat }

default

Returns the command to its default setting of disabled for **sctp-bundle** and 30 seconds for **sctp-heart-beat**.

no

Removes the selected configuration.

sctp-bundle *value*

Specifies that SCTP data chunks are to be queued until this timer expires at which time the data chunks are bundled and committed for transmission. *value* is an integer from 1 through 65535. The granularity is in 100ms increments (10 = 1000ms or 1 second). Default: disabled

sctp-heart-beat *value*

Default: 30 seconds
Specifies the SCTP heartbeat timeout (in seconds) as an integer from 1 through 300. An SCTP heartbeat is sent o a peer to determine reachability. If an acknowledgement is not received before this timer runs out, heartbeat requests are no longer sent and the peer is considered unreachable.

Usage

Use this command to configure timeouts for SCTP data chunk bundle transmissions and/or SCTP heartbeat request responses.

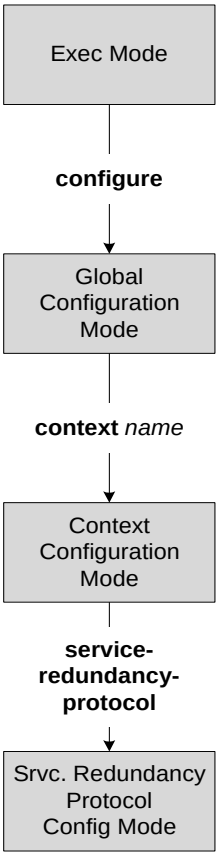
Example

The following command enables the SCTP data chunk bundle timeout value and configures it to 2 seconds:

```
timeout sctp-bundle 20
```

Chapter 248
Service Redundancy Protocol Configuration Mode Commands

The Service Redundancy Protocol Mode is used to configure properties for Interchassis Session Recovery (ICSR) services.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

bind

Binds the service to the IP address of the local chassis.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

bind address { *ipv4 _address* | *ipv6_address* }

no bind address

no

Removes the IP bind address.

ipv4 _address | ipv6_address

Specifies the system IP address using IPv4 dotted-decimal or IPv6 colon-separated notation.

Important: Both peers must be using the same address family (IPv4 or IPv6) or the Service Redundancy Protocol (SRP) connection will not be established.

Usage

Defines the IP address of the local chassis defined as part of the ICSR configuration.

Example

The following example binds the service to the IP address *10.1.1.1*:

```
bind address 10.1.1.1
```

chassis-mode

Defines the chassis's operational mode - primary or backup - for ICSR.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

```
chassis-mode { backup | primary }

default chassis-mode
```

default

Resets the chassis mode to the default setting of backup.

backup

(Default) Configures the system as the backup chassis operating in standby state.

primary

Configures the system as the primary chassis operating in active state.

Usage

Sets the chassis mode (primary or backup) for the system within the framework of ICSR.

Example

The following example configures the system as the primary chassis operating in active state

```
chassis-mode primary
```

checkpoint

Configures check pointing for ICSR. With check pointing enabled, the system stores a snapshot of the current application state use it for restarting the execution in case of failure.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

checkpoint session duration *duration*

default checkpoint session duration

default

Resets the checkpoint session duration to the default setting of 60 seconds.

duration

Specifies the amount of time (in seconds) that a call must be active before it is check pointed. *duration* must be an integer from 1 through 65535.
Default: 60

Usage

Sets the amount of time the chassis waits before check pointing an existing call session.

Example

The following example configures sets the checkpoint session duration to 6500 seconds:

```
checkpoint session duration 6500
```

configuration-interval

Defines the configuration validation interval.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

configuration-interval *interval*

default configuration-interval

default

Resets the configuration interval to the default setting of 3600 seconds.

interval

Specifies the amount of time (number of seconds) between one configuration validation and the next configuration validation.
interval must be an integer from 1 through 65535.
Default: 3600

Usage

This configures the interval between configuration validations of the primary and backup chassis.

Example

The following example sets the configuration interval to 34 seconds:

```
configuration-interval 34
```

dead-interval

Defines the timeout interval before a peer is determined to be down.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

dead-interval *interval*

default dead-interval

default

Resets the dead interval to the default setting of 30 seconds.

interval

Specifies the amount of time (in seconds) for the dead interval. *interval* must be an integer from 1 through 65535.
Default: 30

Usage

This command specifies the amount of time that one chassis waits to receive a communication from a peer before the listening chassis determines that the peer chassis is down.

Example

The following example sets the dead interval to 65 seconds:

```
dead-interval 65
```

delay-interval

Configures the delay time for starting the dead timer after configuration files are loaded.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

delay-interval*interval*

default delay-interval

default

Sets or restores the default value assigned for the specified parameter.

interval

Specifies the amount of time (in seconds) for the delay interval. *interval* must be an integer from 1 through 65535.

Usage

This configures interval for starting the dead timer after configuration files are loaded.

Example

The following example sets the delay interval to 65 seconds after the configuration files are loaded:

```
delay interval 65
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

hello-interval

Defines the lapse time between sending the hello message.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

hello-interval *interval*

default hello-interval

default

Resets the hello interval to the default setting of 10 seconds.

interval

Specifies the lapse time (in seconds) between sending the hello message. *interval* must be an integer from 1 through 65535.
Default: 10

Usage

This command configures the hello interval - the amount of time that lapses between the sending of each hello message. Each chassis sends the other chassis a hello message at the expiration of every hello interval.

Example

The following example sets the hello interval to 35 seconds:

```
hello-interval 35
```

internal-switchover-retry-interval

Defines the interval between internal switchover retries.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

internal-switchover-retry-interval *interval*

default internal-switchover-retry-interval

default

Resets the internal switchover retry interval to the default setting of 60 seconds.

interval

Specifies the amount of time (in seconds) between internal switchover retries. *interval* must be an integer from 10 through 120.
Default: 60

Usage

This configures the interval between internal switchover retries. The system only initiates internal switchovers if Service Redundancy Protocol (SRP) monitoring is configured.

Important: See the **monitor authentication-probe**, **monitor bgp**, or **monitor diameter** commands for more information on associated SRP monitoring.

Example

The following example sets the internal switchover retry interval to 34 seconds:

```
internal-switchover-retry-interval 34
```

monitor authentication-probe

Enables SRP monitoring of the connection between the specified AAA server and the primary chassis.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] monitor authentication-probe context context_name { ipv4_address | ipv6_address }
[ port port_number ]
```

no

Turns off the monitoring.

context *context_name*

Identifies the context being used.
context_name must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

ipv4 _address **|** *ipv6_address*

Defines the IP address of the AAA server to be monitored, entered using IPv4 dotted-decimal or IPv6 colon-separated notation.

port *port_number*

Identifies a specific port for the authentication probe. *port_number* must be the port for the AAA server expressed as an integer from 1 through 65535.

Usage

This command initiates monitoring of the connection between the primary chassis and the specified AAA server through the use of authentication probe packets. If the connection drops, the standby chassis becomes active.

Example

The following example initiates the connection monitoring between the primary chassis and AAA server *10.2.3.4* at port *1025*:

```
monitor authentication-probe context test1 10.2.3.4 port 1025
```

monitor bfd

Enables SRP monitoring of the connection between the specified Bidirectional Forwarding Detection (BFD) neighbor and the primary chassis.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

[no] monitor bfd context *context_name* **{** *ipv4_address* **|** *ipv6_address* **} { chassis-to-chassis | chassis-to-router }**

no

Disables monitoring.

context *context_name*

Identifies the context being used.
context_name must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

ipv4 _address **|** *ipv6_address*

Defines the IP address of the BFD neighbor to be monitored, entered using IPv4 dotted-decimal or IPv6 colon-separated notation

chassis-to-chassis | chassis-to-router

chassis-to-chassis: BFD runs between primary and backup chassis on non-SRP links.
chassis-to-router: BFD runs between chassis and router.

Usage

This command initiates monitoring of the connection between the primary chassis and the specified BFD neighbor in the specified context. If the connection drops, the standby chassis becomes active.

Important: BFD monitoring must run between chassis-to-chassis or chassis-to-router.

Example

The following example initiates the chassis-to-chassis connection monitoring between the primary chassis and BFD neighbor *12.2.1.54*:

```
monitor bfd context test 12.2.1.54 chassis-to-chassis
```

monitor bgp

Enables SRP monitoring of the connection between the specified Border Gateway Protocol (BGP) peer and the primary chassis.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

[no] monitor bgp context *context_name* **{** *ipv4_address* **|** *ipv6_address* **} [vrf** *vrf_name* **]**

no

Disables monitoring.

context *context_name*

Identifies the context being used.
context_name must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

ipv4 _address **|** *ipv6_address*

Defines the IP address of the BGP peer to be monitored, entered using IPv4 dotted-decimal or IPv6 colon-separated notation

vrf *vrf_name*

Defines the VPN Routing/Forwarding instance.

Usage

This command initiates monitoring of the connection between the primary chassis and the specified BGP peer in the specified context. If the connection drops, the standby chassis becomes active.

Example

The following example initiates the connection monitoring between the primary chassis and BGP peer *125.2.1.56*:

```
monitor bgp context test 125.2.1.56
```

monitor diameter

Enables SRP monitoring of the connection between the specified Diameter server and the primary chassis.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

[no] monitor diameter context *context_name* **endpoint** *endpoint_name* **[fqdn** *fqdn* **| peer {** *ipv4_address* **|** *ipv6_address* **}] [port** *port_number* **]**

no

Turns off the monitoring.

context *context_name*

Identifies the context being used.
context_name must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

endpoint *endpoint_name*

Identifies the endpoint being used.
endpoint_name must be for the Diameter server expressed as an alphanumeric string of 1 through 63 characters.

fqdn *fqdn*

Identifies a Fully Qualified Domain Name (FQDN).
fqdn must be for the Diameter server expressed an alphanumeric string of 1 through 127 characters.

peer { *ipv4 _address* **|** *ipv6_address* **}**

Defines the IP address of the Diameter server to be monitored, entered using IPv4 dotted-decimal or IPv6 colon-separated notation.

port *port_number*

Identifies a specific port to monitor.
port_number must be the port for the Diameter server and an integer from 1 through 65535.

Usage

This command initiates monitoring of the connection between the primary chassis and the specified Diameter server in the specified context. If the connection drops, the standby chassis becomes active.

Important: Endpoint name, FQDN, IP address, and port must all match the Diameter protocol configured values for the peer state to be updated.

Example

The following example initiates the connection monitoring between the primary chassis and the Diameter server on context *test1* and endpoint *end2*:

```
monitor diameter context test1 10.6.7.8 endpoint end2
```

num-internal-switchover-retry

Defines the number of times an internal switchover would be retried.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

num-internal-switchover-retry *retries*

default num-internal-switchover-retry

default

Resets the configuration interval to the default setting of 3 retries.

retries

The number of times an internal switchover would be retried in case of standby chassis. *retries* must be an integer from 1 through 10.
Default: 3

Usage

This configures the number of times an internal switchover would be retried in case of standby chassis failure to respond or become active.

Example

The following example sets the retry number to *5*:

```
num-internal-switchover-retry 5
```

peer-ip-address

Specifies the IP address for the peer chassis.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

```
peer-ip-address { ipv4_address | ipv6_address }

no peer-ip-address
```

no

Removes the peer IP address of the backup chassis.

ipv4_address | *ipv6_address*

Specifies the IP address of the backup chassis, entered using IPv4 dotted-decimal or IPv6 colon-separated notation.

Important: Both peers must be using the same address family (IPv4 or IPv6) or the Service Redundancy Protocol (SRP) connection will not be established.

Usage

This command is used to identify the peer chassis in the ICSR configuration. From the primary's perspective, the peer is the backup and from the backup's perspective, the peer is the primary.

Example

The following example specifies *10.2.3.4* as a backup peer system to the primary system:

```
peer-ip-address 10.2.3.4
```

priority

Sets the initial ICSR priority of each peer chassis.

Important: **priority** takes affect only during simultaneous initializing of all chassis in an ICSR configuration, and only if a misconfiguration has both chassis in the same mode (both Primary or both Backup).

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

priority *priority_value*

default priority

default

Resets the priority to the default setting of 125.

priority_value

Specifies the priority for the chassis.
priority_value must be an integer from 1 through 255, where 1 is the highest priority.
Default: 125

Usage

This command determines which chassis transitions to the Active state when all chassis have the same mode configuration. **priority** acts as a tie breaker for the state determination only when all chassis initialize simultaneously. The chassis with the higher priority (lower number) becomes Active, while the chassis with the lower priority (higher number) becomes Standby.
Once chassis become operational (after initialization), if there is an event requiring a chassis change of state, then each chassis returns to its previous state (Active or Standby) after both chassis recover.

Example

The following example sets the priority value to *5*:

```
priority 5
```

route-modifier

Sets the route modifier for the peer chassis.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Syntax

route-modifier threshold *threshold_value*

default route-modifier

default

Resets the route modifier to the default setting of 16.

threshold_value

Specifies the value that causes the route-modifier counter to be reset to the initial value. *threshold_value* must be an integer from 2 through 32.
Default: 16

Usage

This command is used to determine when the route modifier should be reset to its initial value to avoid rollover.

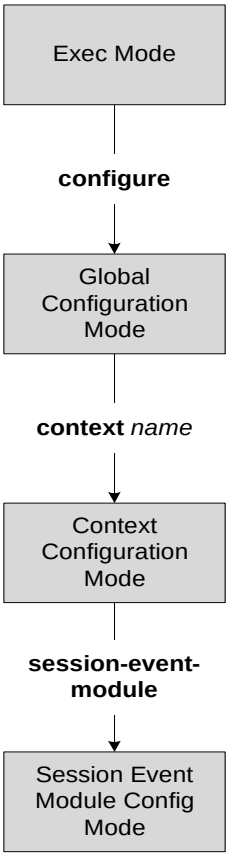
Example

The following example sets the route modifier threshold to *10*:

```
route-modifier threshold 10
```

Chapter 249
Session Event Module Configuration Mode Commands

The Session Event Module Configuration Mode is used to configure how subscriber-specific event data is handled on the S-GW. As users attach, detach, and move through the network, they trigger signaling events that need to be recorded. To provide a per-subscriber level of reporting, the S-GW sends a stream of user event data to an event reporting server over SFTP.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

event

Sets the method and destination for transferring event files.

Product

S-GW

Privilege

Administrator

Syntax

event { purge { storage-limit *bytes* **| time-limit** *seconds* **} | push-interval** *value* **| push-trigger space-usage-percent** *trigger_percentage* **| remove-file-after-transfer | transfer-mode { pull [module-only] | push primary { encrypted-url** *encrypted_url* **| url** *url* **} [max-files** *files* **] [module-only] [secondary { encrypted-secondary-url** *url* **| secondary-url** *url* **}] [via local-context] } | use-harddisk }**

default event [purge | push-interval | push-trigger space-usage-percent | remove-file-after-transfer | transfer-mode | use-harddisk]

no event [purge | remove-file-after-transfer | use-harddisk]

---

default

Configures the default setting for the specified keyword(s):

- **purge**: Not enabled.
- **push-interval**: 60 seconds
- **push-trigger**: 80 percent
- **remove-file-after-transfer**: Disabled
- **transfer mode**: Push
- **use-harddisk**: Disabled

---

no

Disables the configured event file storage and processing in this mode:

- **purge**: Disables the deleting of record files on the hard disk based on a storage limit or a time limit.
- **remove-file-after-transfer**: Retains a copy of the file even after it has been pushed or pulled to another server.
- **use-harddisk**: Disables data storage on the system's hard disk.

---

purge { storage-limit *bytes* **| time-limit** *seconds* **}**

Configures parameters for deleting event records from the hard drive. This command is not enabled by default.
storage-limit *bytes*: Specifies that event records are to be deleted from the hard drive upon reaching a storage limit defined in bytes. *bytes* must be an integer value from 10485760 to 146800640.
time-limit *seconds*: Specifies that event records are to be deleted from the hard drive upon reaching a time limit defined in seconds. *seconds* must be an integer value from 600 to 2592000.

push-interval *value*

Default: 60
Specifies the transfer interval (in seconds) when event files will be pushed to an external file server. *value* must be an integer from 30 through 3600.

push-trigger space-usage-percent *trigger_percentage*

Default: 80
Specifies the disk space utilization percentage threshold at which an automatic push is triggered and files are transferred to the external server. *trigger_percentage* must be an integer from 10 through 80.

remove-file-after-transfer

Default: Disabled
Specifies that the system must delete event files after they have been transferred to the external file server.

transfer-mode { pull [module-only] | push primary { encrypted-url *encrypted_url* **| url** *url* **} [max-files** *files* **] [module-only] [secondary { encrypted-secondary-url** *url* **| secondary-url** *url* **}] [via local-context] }**

Specifies the transfer mode to be used when transferring event files to an external file server.

- **pull**: Specifies that the destination server will pull the event files.
- **push**: Specifies that the system will push event files to the destination server. This is the default mode.
- **primary encrypted-url** *encrypted_url*: Specifies the primary URL location to which the system pushes the files in encrypted format. *encrypted_url* must be an alphanumeric string of 1 through 8192 characters.
- **primary url** *url*: Specifies the primary URL location to which the system pushes the event files. *url* must be an alphanumeric string of 1 through 1024 characters in the format: *//user:password@host:[port]/direct*.
- **max-files** *number*: Specifies the maximum number of files that can be transferred per push. *number* must be an integer from 4 to 4000.
- **module-only**: Specifies that the transfer of event records is to be applied only to the module type for which the configuration was originally created. If this option is not enabled, the transfer will occur for all record types.
- **secondary encrypted-secondary-url** *url*: Specifies the secondary URL location to which the system pushes the files in encrypted format. *url* must be an alphanumeric string of 1 through 8192 characters.
- **secondary-url** *url*: Specifies the secondary URL location to which the system pushes the event files. *url* must be an alphanumeric string of 1 through 1024 characters in the format: *//user:password@host:[port]/direct*
- **via local-context**: Specifies that the local context, and, subsequently, the SPIO management ports, will be used to pull or push event files from/to the event server.

use-harddisk

Default: Disabled
Specifies that the hard disk drive on the SMC is to be used to store S-GW event records.

Usage

Use this command to configure how the S-GW event records are moved and stored. By default, records are stored in the PSC RAM where the CDRMOD instance is running.

The **event use-harddisk** command can be run only in a context where CDRMOD is running. Configuring in any other context will result in failure with the message "Failure: Please Check if CDRMOD is running in this context or not."

If push transfer mode is configured, the server URL to which the event files will be transferred must be specified.

When changing the transfer-mode from pull to push, disable the pull setting before changing the transfer mode to push. The push to server URL must be accessible from the local context. Also, make sure that its base directory contains an **event** subdirectory.

After changing the transfer mode from push to pull, enable pull on the destination server. Any ongoing push activity will continue until all the file transfers are completed. If there is no ongoing push activity at the time of this configuration change, the push-related configuration is nullified immediately.

Example

The following command sets the space usage trigger for pushing files to the event server to 60%:

```
event push-trigger space-usage-percent 60
```

The following command specifies that the event files are to be transferred to a server with the URL of user:password@event-server.com:

```
event transfer-mode push primary url //user:password@event-server.com
```

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

file

Sets the format and handling characteristics of event files.

Product

S-GW

Privilege

Administrator

Syntax

file [compression { gzip | none }] [current-prefix *string* **] [delete-timeout** *seconds* **] [directory** *directory_name* **] [exclude-checksum-record] [field-separator { hyphen | omit | underscore }] [file-sequence-number rulebase-seq-num] [headers] [name** *file_name* **] [reset-indicator] [rotation [num-records** *number* **| time** *seconds* **| volume** *bytes* **]] [sequence-number { length** *length* **| omit | padded | padded-six-length | unpadded }] [storage-limit** *limit* **] [time-stamp { expanded-format | rotated-format | unix-format }] [trailing-text** *string* **] [trap-on-file-delete] [xor-final-record] +**

default file [compression] [current-prefix] [delete-timeout] [directory] [field-separator] [file-sequence-number] [headers] [name] [reset-indicator] [rotation { num-records | time | volume }] [sequence-number] [storage-limit] [time-stamp] [trailing-text] +

default

Configures the default setting for the specified keyword(s).

compression { gzip | none }

Specifies compression of S-GW event files.

- **gzip**: Enables GNU zip compression of the event file at approximately 10:1 ratio.
- **none**: Disables Gzip compression.

current-prefix *string*

Specifies a string to add to the beginning of the event file that is currently being used to store records. *string* must be an alphanumeric string of 1 through 31 characters. Default: **curr**

delete-timeout *seconds*

Specifies a time period, in seconds, after which event files are deleted. By default, files are never deleted. *seconds* must be an integer from 3600 through 31536000. Default: Disabled

directory *directory_name*

Specifies a subdirectory in the default directory in which to store event files. *directory_name* must be an alphanumeric string of 1 through 191 characters. Default: **/records/event**

exclude-checksum-record

Excludes the final record containing #CHECKSUM followed by the 32-bit Cyclic Redundancy Check (CRC) of all preceding records from the event file.

Default: Disabled, a checksum record is included in the event file header.

field-separator [hyphen | omit | underscore]

Specifies the type of separators between two fields of an event file name:

- **hyphen**: Specifies the field separator as a "-" (hyphen) symbol between two fields.
- **omit**: Removes or omits the field separator between two fields.
- **underscore**: Specifies the field separator as an "_" (underscore) symbol between two fields.

file-sequence-number rulebase-seq-num

Specifies that the file name sequence numbers be unique per rulebase and event format name combination.

headers

Includes a file header summarizing the record layout.

name *file_name*

Specifies a string to be used as the base file name for event files. *file_name* must be an alphanumeric string of 1 through 31 characters. The file name format is as follows:
base_sequencenum_timestamp Default: **event**

- *base*: Specifies type of record in file or contains the operator-specified string. Default: **event**
- *sequencenum*: This is a 5-digit sequence number to detect the missing file sequence. It is unique among all event files on the system.
- *timestamp*: Adds a file creation timestamp (UTC time) in MMDDYYYYHHMMSS format.

reset-indicator

Specifies the inclusion of the reset indicator counter (value from 0 through 255) in the event file name. The counter is incremented whenever any of the following conditions occur:

- A peer chassis has taken over in compliance with Interchassis Session Recovery (ICSR).
- The sequence number (see **sequence-number** keyword) has rolled over to zero.

rotation { num-records *number* **| time** *seconds* **| volume** *bytes* **}**

Specifies when to close an event file and create a new one.

- **num-records** *number*: Specifies the maximum number of records that should be added to an event file. When the number of records in the file reaches this value, the file is complete. *number* must be an integer 100 through 10240. Default: 1024
- **time** *seconds*: Specifies the period of time to wait (in seconds) before closing the current event file and creating a new one. *seconds* must be an integer from 30 through 86400. Default: 3600
- **volume** *bytes*: Specifies the maximum size of the event file (in bytes) before closing it and creating a new one. *bytes* must be an integer from 51200 through 62914560. Note that a higher setting may improve the compression ratio when the compression keyword is set to gzip. Default: 102400

sequence-number { length *length* **| omit | padded | padded-six-length | unpadded }**

Includes with a specified format or excludes the sequence number in the file name.

- **length** *length*: Includes the sequence number with the specified length. *length* must be the file sequence number length with preceding zeroes in the file name, and must be an integer from 1 through 9.

- **omit**: Excludes the sequence number from the file name.
- **padded**: Includes the padded sequence number with preceding zeros in the file name. This is the default setting.
- **padded-six-length**: Includes the padded sequence number with six preceding zeros in the file name.
- **unpadded**: Includes the unpadded sequence number in the file name.

Default: **padded**

---

storage-limit *limit*

Files will be deleted when the specified amount of space (in bytes0 is reached.
limit must be an integer from 10485760 through 536870912. Default: 33554432

---

time-stamp { expanded-format | rotated-format | unix-format }

Specifies the format of the file creation timestamp to be included in the file name.

- **expanded-format**: Specifies the UTC (Universal Time Coordinated) MMDDYYYYHHMMSS format.
- **rotated-format**: Specifies the time stamp format to YYYYMMDDHHMMSS format.
- **unix-format**: Specifies the UNIX format of *x.y*, where *x* is the number of seconds since 1/1/1970 and *y* is the fractional portion of the current second that has elapsed.

---

trailing-text *string*

Specifies the inclusion of an arbitrary text string in the file name as an alphanumeric string of 1 through 30 characters.

---

trap-on-file-delete

Instructs the system to send an SNMP notification (trap) when an event file is deleted due to lack of space. Default: Disabled

---

xor-final-record

Specifies inserting an exclusive OR (XOR) checksum (instead of a CRC checksum) into the event file header if the **exclude-checksum-record** is left at its default setting. Default: Disabled

---

+

More than one of the previous keywords can be entered within a single command.

Usage

Use this command to configure event file characteristics.

Example

The following command sets the prefix of the current active event file to *Current*:

```
file current-prefix Current
```

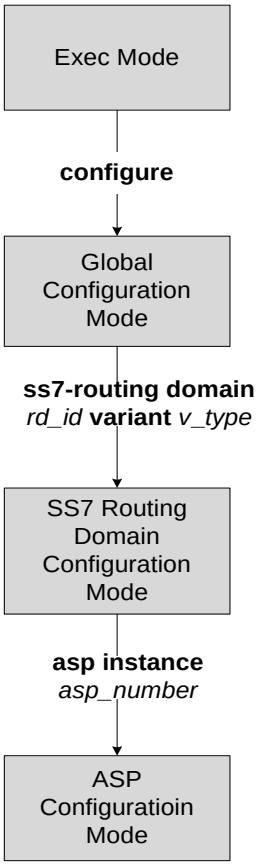
The following command sets the base file name to *Eventfile*:

```
file name Eventfile
```

Chapter 250
SGSN ASP Configuration Mode Commands

The ASP (application server process) configuration mode defines the M3UA end-point parameters for a specific SS7 routing domain instance. The ASP instance is generated and accessed via the SS7 routing domain configuration mode commands.

`[local]`*`hostname`*`(config-ss7-rd-<`*`ss7rd_id`*`>-asp-inst-<`*`asp_inst`*`>)#`



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current mode and returns to the Exec Mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec Mode.

end-point

This command defines or deletes the IP address and/or port number to be associated with the local SCTP end-point for this ASP. At least one address needs to be configured before the end-point can be activated.

When using the **bind** keyword, this command also activates the end-point once the address has been defined. Once bound, it cannot be reconfigured until it is unbound with the **no end-point bind** command.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end-point { address ip_address context context_id | bind | port port_number }

no end-point { address ip_address context context_id | bind }
```

address ip_address context context_id:

Specifies the IP address and the context associated with the address for this end-point.
ip_address**:** must be defined using the standard IPv4 dotted decimal notation or the colon notation of IPv6.
context context_id: a string of 1 to 79 alphanumeric characters to identify the specific context associated with the end-point address.

bind

Activates (binds) the end-point.

Important: Only use **bind** after you have configured other parameters.

port port_number

Identifies the M3UA's SCTP port associated with this end-point.
port_number: must be an integer fom 1 to 65535. Default is 2905.

no

Removes the end-point configuration or deactivates the end-point.

Caution: Entering this command will terminate all current subscriber sessions for associated peers.

Usage

Use this command to manage the ASP end-point. Once the ASP end-point is bound the end-point configuration can not be changed until it is unbound.

Example

Activate the end-point with the following command:

```
end-point bind
```

Deactivate or unbind the end-point with the following command:

```
no end-point bind
```

Set the end-point port to default for ASP 1 with the following command:

```
default asp instance 1 end-point port
```

exit

Exits the current mode and returns to the previous mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Returns to the previous mode.

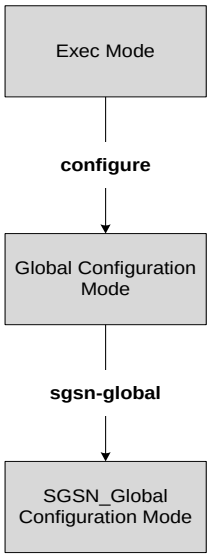
Chapter 251
SGSN Global Configuration Mode Commands

The commands in this mode configure SGSN-specific parameters impact the entire SGSN and that are independent of the GPRS or the IuPS services.

In this mode, your prompt will look similar to:

```
[local]hostname(config-sgsn-global)#
```

The SGSN Global configuration mode is a sub-mode derived from the Global configuration mode.



aggregate-ipc-msg

Enables/disables aggregation of inter-process communication (IPC) messages in the link manager (linkmgr) and session manager (sessmgr).

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

aggregate-ipc-msg { linkmgr | sessmgr } { flush-frequency *frequency* **| num-msgs** *number_msgs* **}**

default aggregate-ipc-msg { linkmgr | sessmgr }

default

Resets the managers to default values for flushing.

linkmgr

Selects the linkmgr to configure the number of IPC messages to be aggregated and frequency of flushing.

sessmgr

Selects the sessmgr to configure the number of IPC messages to be aggregated and frequency of flushing.

flush-frequency *frequency*

Configure the frequency, in 100-millisecond intervals, that the aggregated IPC messages will be flushed.
frequency : Enter an integer from 1 to 3. Default is 1.

num-msgs *number_msgs*

Configure the number of IPC messages to aggregate before flushing.
number_msgs : Enter the integer 1 (to disable aggregation) or an integer from 2 to 164 to define the number of messages. Default is 10.

Usage

Use this command to enable/disable aggregation of IPC messages in the linkmgr and/or the sessmgr. This command includes options to configure the frequency of aggregated message flushing and the number of packets to be buffered before the flush.
At the HNB-GW node this command provides the solution to reduce the latency while sending the IPC messages towards core network (CN).
In default scenario on HNB-GW the Link manager buffers the packets and then send it over SCCP link if there are events to be sent SCCP Connection Request (SCCP CR) towards Core node side. It aggregate packets for 100 msec and send it with whatever aggregation it has done in those 100 msecs.
At the HNB-GW this command can be used to reduce the processing of sending every individual events out on the wire towards core node side from HNB-GW in following manner:

- If this aggregation is enabled, then there could be time delay seen on the wire for sending SCCP CR depending on configuration of HNB-GW.
- If this aggregation is reduced to 1 (that means as soon as there is event to send out namely SCCP CR is available to send out on the wire), it will be immediately seen on the wire and SCCP connection setup time is reduced because of immediate sending of SCCP CR and not waiting for aggregation.

To view aggregate IPC message statistics, use command **show config | grep aggregate-ipc-msg**.

Example

Configure the linkmgr to buffer *45* messages before flushing the linkmgr IPC messages:

```
aggregate-ipc-msg linkmgr flush-frequency 45
```

On HNB-GW the following command configures the *linkmgr* to flush the IPC messages towards CN without aggregation:

```
aggregate-ipc-msg linkmgr1
```

On HNB-GW the following command configures the *sessmgr* to flush the IPC messages towards CN without aggregation:

```
aggregate-ipc-msg sessmgr 1
```

apn-resolve-dns-query snaptr

Enable/disable sending of SNAPTR DNS query to resolve an APN for a subscriber with an EPS (evolved packet system)-capable handset.

Important: This command is no longer available in all 12.0 and 12.2 releases. If you do not see this command in your release, look for the **apn-resolve-dns-query snaptr** command in the APN Profile configuration mode to accomplish the same task.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] apn-resolve-dns-query snaptr

default apn-resolve-dns-query
```

default

Resets the default, the ability to send SNAPTR DNS query is disabled.

no

Disables the ability to send SNAPTR DNS query.

Usage

By default, sending the SNAPTR DNS query is disabled. Use this command to send SNAPTR DNS query when resolving an APN for an EPS-capable subscriber.
At PDP context activation, the SGSN will use the UE capabilitly as input to select either a GGSN or a P-GW for the EPS-capable subscriber. The SNAPTR DNS query will be used for P-GW resolution. Enabling this feature will give priority to P-GW selection for E-UTRAN-capable UEs.

Example

Use the following command to enable sending of SNAPTR DNS query for APN resolution:

```
apn-resolve-dns-query
```

Use the following command to disable the use of SNAPTR DNS query for APN resolution:

```
no apn-resolve-dns-query
```

bssgp-message ms-flow-control-from-unknown-ms

This command determines the SGSN response to MS-Flow-Control messages received from an unknown MS.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
bssgp-message ms-flow-control-from-unknown-ms { discard-message | send-ack | send-status
}

default bssgp-message ms-flow-control-from-unknown-ms
```

default

Including **default** with the command configures the SGSN to use default behavior so that the SGSN sends BSSGP-Status messages whenever the SGSN receives an MS-Flow-Control message from an unknown MS.

discard-message

This keyword instructs the SGSN to discard the received BSSGP message. With this option, the SGSN does not send any response to the MS after discarding the received BSSGP message.

send-ack

This keyword instructs the SGSN to send an acknowledgement message (MS-Flow-Control-ACK) after receiving an MS-Flow-Control message.

send-status

Default
This keyword instructs the SGSN to send a BSSGP-Status message to the MS whenever the SGSN receives an MS-Flow-Control message from an unknown MS.

Usage

This command allows the operator to specify the action the SGSN needs to take whenever the SGSN receives an MS-Flow-Control message from an unknown mobile station. This configuration determines the response for the SGSN globally.
The list of possible actions are:

- send a BSSGP-Status response message
- send an ACK message (MS-Flow-Control-ACK)
- discard the BSSGP message

To see the statistics for the number of MS-Flow-Control messages that have been discarded, use the **show bssgp statistics** command from the Exec mode.

Example

Change the default configuration and have the SGSN acknowledge receipt of the MS-Flow-Control message:

```
bssgp-message ms-flow-control-from-unknown-ms send-ack
```

bssgp-message ptp-bvc-reset

This command determines the SGSN response, per BVCI, to receipt of a peer-to-peer BVC Reset.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
bssgp-message ptp-bvc-reset { frc-subscriber-standby | retain-current-state }

default bssgp-message ptp-bvc-reset
```

default

Including **default** with the command configures the SGSN to use default behavior so that the SGSN continues with the current state once a peer-to-peer BVC Reset is received.

frc-subscriber-standby

This keyword instructs the SGSN to change the state of the subscribers to standby when the peer-to-peer BVC Reset is received.

retain-current-state

Default
This keyword instructs the SGSN to continue the current state of the subscribers when the BVC Reset message is received.

Usage

This command allows the operator to specify the action the SGSN needs to take whenever the SGSN receives a peer-to-peer BVC Reset message for a specific BVCI.
To confirm the configuration for the response to the BVC Reset, use the **show sgsn-mode** command from the Exec mode.

Example

Change the default configuration and have the SGSN change subscriber states to standby:

```
bssgp-message ptp-bvc-reset frc-subscriber-standby
```

bssgp-timer

Configures the T2 and TH timers for the BVCs (BSSGP virtual connections) of the NSE (network service entities).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
bssgp-timer { t2 T2_time | th TH_time }

default bssgp-timer { t2 | th }
```

default

Resets the specified timers to default settings.

t2 *T2_time*

Configures the BVC reset guard timer (at the BSSGP layer) in units of 1 second.
T2_time : Enter an integer from 1 to 120. Default is 30 seconds.

th *TH_time*

Configures, at the BSSGP layer, the MS flow control parameter validity timeouts in units of 1 second.
TH_time : Enter an integer from 6 to 5999. Default is 500 seconds.

Usage

Use this command to configure timer timeout values for MS flow control and BVC reset timers that control BVCs for the NSEs.

Example

Set the TH timeout for *20* seconds:

```
bssgp-timer th 20
```

bvc-unblock

This command enables (disabled by default) or disables the SGSN to unblock blocked BVCs based on the receipt of uplink packets from the BSC.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
bvc-unblock { data-or-flow-control | flow-control | ul-data }

[ default | no ] bvc-unblock
```

default

Include **default** with the command to disable the function.

no

Include **no** with the command to disable this function.

data-or-flow-control

Enables the BVC-Unblock function when the SGSN receives either a FLOW-CONTROL-BVC packet or a UL-UNITDATA packet.

flow-control

Enables the BVC-Unblock function when the SGSN receives a FLOW-CONTROL-BVC packet.

ul-data

Enables the BVC-Unblock function when the SGSN receives a UL-UNITDATA packet.

Usage

Configurations defined with this command are common to all NSE defined for the SGSN.
This command is useful if there is a BVC status mismatch across different SGSN managers (such as the sessmgr and the linkmgr) when the BSC sends BVC-Block (SGSN should move to BLOCKED) followed by a BVC-Reset (SGSN should move to UNBLOCKED). Such mismatches can easily occur, particularly on Gb-IP network connection, when one link receives the BVC-Block and a different link receives the BVC-Reset with little delay between the two.
If BVC-Unblock function is enabled, the SGSN ensures that BVCs which are in the BLOCKED state move to the UNBLOCKED state upon receipt of the configured packet type(s).

Example

Instruct the SGSN to perform BVC-Unblock when a mismatch occurs and the SGSN receives a FLOW-CONTROL-BVC packet:

```
bvc-unblock flow-control
```

dscp-template

Creates and/or deletes DSCP templates that can be configured for use for all GPRS services on the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

dscp-template *template_name* **[-noconfirm]**

no dscp-template *template_name*

no

Deletes the template instance from the SGSN Global configuration.

template_name

Enter 1 to 64 alphanumeric characters, including dots (.), dashes (-), and forward slashes (/). to identify a unique instance of a DSCP template.
There is no known limit to the number of templates that can be created.

Usage

This command enables the operator to create or delete an instance of a DSCP template. The DSCP templates are used to define the DSCP configuration for control packets and data packets for the GPRS services.
Related commands:

- This command provides access to the mode containing all the configuration commands used to define DSCP markings for the control packets and data packets for a particular GPRS service (see the *DSCP Template Configuration Mode Commands* section).
- To associated a specpific DSCP template with a specific GPRS service configuration, use the **associate-dscp-template downlink** documented in the *GPRS Service Configuration Mode Commands* section.
- To check the list of DSCP templates configured, use the **show sgsn-mode** command documented in the *Exec Mode Commands* section.

Example

Use a command similar to the following to create a DSCP template with ID *dscp_london* that can be used specifically for Gb/IP calls from subscribers in London:

```
dscp-template dscp_london
```

dual-address-pdp

This command makes it possible for the operator to enable (default) / disable SGSN support for MS requests for dual PDP type (IPv4v6) addressing.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] dual-address-pdp
```

default

Enables dual PDP type address support.

no

Disables the default behavior so that the SGSN does not honor requests for dual PDP type addresses.

Usage

With release 12.2 and in accordance with 3GPP Release 9.0 specifications, by default the SGSN honors the MS/UE request for dual PDP type addressing (IPv4v6) for PDP context association with one IPv4 address and one IPv6 address/prefix. This support can be disabled by configuration.

Important: For the dual PDP addressing feature to function, **common-flags** must be enabled with the **gptc send** command in the SGTP service configuration mode *prior* to enabling the feature with the **dual-address-pdp** command.

With this default behavior, the operator has multiple options to refine the level of support for dual PDP type addressing through the use of several related commands.

- **dual-address-pdp** command in the RNC configuration mode disables SGSN support for dual PDP type addressing for a specific RNC that either does or does not support this type of addressing..
- **pdp-type-ipv4v6-override** in the APN profile configuration mode allows the SGSN to override the MS/UE request for dual PDP type addressing.
- Using the **dual-ipv4v6** keyword with the **wildcard-apn pdp-type** command in the APN remap table configuration mode enables the operator to configure a default APN with a wildcard subscription with PDP type IPv4v6.

Example

Use the following command to disable support for dual PDP type addressing (IPv4v6):

```
no dual-address-pdp
```

If dual PDP addressing has been disabled, to renable the feature, move to the SGTP service configuration mode, in the appropriate context, to perform the following as the *first* command needed to re-enable support for dual PDP type addressing in the configuration:

```
gtpc send common-flags
```

Now in the SGSN global configuration mode, use the following as the second command required to re-enable support for dual PDP type addressing in the configuration:

```
dual-address-pdp
```

end

Exits the current mode and returns to the Exec Mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Change the mode back to the Exec Mode.

exit

Exits the current mode and returns to the previous configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Change the mode to the Global Configuration Mode.

gmm-message

This command configures the SGSN to discard (drop) the Attach-Request message received with a random TLLI already in use.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default ] gmm-message attach-with-tlli-in-use discard-message
```

default

Resets the default function allowing multiple MS, using the same random TLLI, to attempt to Attach simultaneously and disables discarding the Attach-Request message for random TLLI already in use.

Usage

Working with the two related commands (noted below), this command is part of a procedure for handling multiple MS Attaches all with the Same Random TLLI. Use this command to configure the SGSN to allow only one subscriber at a time to attach using a fixed random TLLI.

Related Commands:

- The **old-tlli invalidate tlli** command configures a list of random TLLI to be invalidated from the GMM after the invalidate old-TLLI timer expires.
- The **old-tlli hold-time** command configures the old-TLLI expiry timer.

Example

Configure the SGSN to drop Attach Request containing TLLI already in use:

```
gmm-message attach-with-tlli-in-use discard-message
```

imsi-range

Configure an IMSI range or a PLMN ID to associate with an Operator Policy.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

imsi-range mcc *mcc_num* **mnc** *mnc_num* **{ msin first** *start_number* **last** *stop_number* **[operator-policy** *policy_name* **[description** *description* **]] | plmnid** *plmn_id* **operator-policy** *policy_name* **[description** *description* **] } +**

no imsi-range mcc *mcc_num* **mnc** *mnc_num* **{ msin first** *start_number* **last** *stop_number* **| plmnid** *plmn_id* **}**

---

no

Using **no** in the command deletes the definition from the SGSN Global configuration.

---

mcc *mcc_num*

mcc defines the mobile country code (MCC) of an IMSI.
mcc_num: Enter a 3-digit number from 100 to 999 - 000 to 099 are reserved.

---

mnc *mnc_num*

mnc defines the mobile network code (MNC) of an IMSI.
mnc_num: Enter a 2 or 3-digit number from 00 to 999.

---

msin

MSIN (mobile subscriber international number) portion of the IMSI.
first *start_num:* Defines first MSIN prefix number in a range
last *stop_num:* Defines the last or final MSIN prefix number in a range.

---

operator-policy *policy_name* **description** *description*

Identify the operator policy that the IMSI range definition and/or the PLMN-ID is to be associated.
policy_name : Enter a string of 1 to 64 alphanumeric characters.
description: Enter a string of 1 to 100 alphanumeric characters to provide range clarification for converted Release 9.0 configurations.
If a PLMN-ID is to be included in the definition, enter the **plmnid** before entering the operator policy name.

---

plmnid *plmn_id*

The 5-6 digit PLMN-ID consists of the MCC (mobile country code) plus the MNC (mobile network code) to identify the public land mobile network (PLMN) for a specific operator. This keyword associates a specific PLMN with this specific SGSN operator policy.
plmn_id : Enter 5 to 6 digits.

+

This symbol indicates that command can be repeated to create repeated definitions.

Usage

An IMSI = maximum of 15 digits. An IMSI consists of the MCC (3 digits) + the MNC (2 or 3 digits) + the MSIN (the remaining 10 or 9 digits depending on the length of the MNC).
MCC and MNC are the minimum amount of information required to identify a unique operator policy with IMSI filtering. The MCC and MNC combine uniquely to identify the country and the network operator, for example: Cingular Wireless in the United States = **mcc** *311***mnc** *180*
To improve the granularity of call handling, an operator policy with additional IMSI filtering parameters can be defined, to include filtering based on the MSIN, by defining a MSIN range - first (or start-of-range) MSIN and last (or end-of-range) MSIN. The range numbers do not include the maximum allowed for the MSIN but should include a sufficient number to enable the operator policy to filter effectively.
For the most efficient IMSI filter, the operator policy should include all of the above parameters and the PLMN ID which defines the current location of the MS -- this parameter is particularly useful for highlighting which calls are roaming.
And if none of the operator policies contain useful filtering information, then the default operator policy will be applied as the information in this command is never defined for the default operator policy.
The following table will illustrate how these filtering parameters determine which operator policy will govern a call:

Operator Policy ID	MCC	MNC	MSINfirst	MSINlast	PLMN ID
OpPol-1	123	45	67890	67898	
OpPol-2	123	45			
OpPol-3	123	45	67890	67898	23232
OpPol-4	123	45			23232
OpPol-5	123	45	6789012	6789019	
OpPol-6	123	45	6789012	6789019	23232
default					

The filtering selects which operator policy will be used to determine how a call is handled - the operator policy that best matches the IMSI. So, a call with IMSI 123456789012345 PLMNID 23232 is best matched with OpPol-6.
In most cases, the operator policy with the most information defined will be used as a combination of PLMNID and IMSI provides the best match. But OpPol-6 won't always be the best match. Using the table above:
OpPol-1 is the best match for IMSI 123456789011111
OpPol-2 is the best match for IMSI 123456789099999
OpPol-5 is the best match for IMSI 123456789012345 if the PLMNID is 12344

Example

The following associates operator policy *oppol1* with country code *310*, mobile network code of *33*, and IMSI range *1231234 - 1231244*:

```
imsi-range mcc 310 mnc 33 msin first 1231234 last 1231244 operator-policy
oppol1
```

map-message

This command instructs the SGSN to ignore the CAMEL subscription when there is no CAMEL service associated or in existence.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
map-message insert-subscriber-data csi-handling when-camel-not-associated ignore-subscription

default map-message insert-subscriber-data csi-handling
```

default

Resets the SGSN's default behavior. By default, the SGSN validates the CAMEL subscription and rejects an Attach Request when there is no CAMEL service association.

Usage

By default, the SGSN updates the the CAMEL subscription included in the INSERT-SUBSCRIBER-DATA (ISD) messages received from the HLR. While processing the ATTACH request from the CAMEL subscriber, the SGSN checks whether it has a CAMEL service associated with the corresponding service (either GPRS service or SGN service). It drops the ATTACH request if there is no CAMEL service associated with a corresponding service.
Also by default, the SGSN does not allow establishment of a Direct Tunnel (DT) for a CAMEL subscriber. It strictly validates the subscriber against the CAMEL subscription during the Direct Tunnel setup procedure. This command enables the operator to control the behavior of the SGSN by configuring the SGSN to ignore the CAMEL subscription. This allows the SGSN to successfully complete an ATTACH procedure when there is an ATTACH Request from a CAMEL subscriber and there is no CAMEL service association in the SGSN. As well, during the Direct Tunnel establishment, validation of the CAMEL subscription is ignored to allow the DT to setup when there is no CAMEL service association in the SGSN.

Example

Instruct the SGSN to validate the CAMEL subscription:

```
default map-message insert-subscriber-data csi-handling
```

max-pending-attaches

Configure the maximum length of the pending attach queue.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

max-pending-attaches *limit*

default max-pending-attaches

default

Resets the SGSN's Attach queue to a maximum pending value of 10,000.

limit

Set the a maximum limit to the pending Attach/RAU messages queue in the LinkMgr. When the limit is reached a message is sent to the IMSIMgr.
limit : Enter an integer from 5000 - 50000. Default is 10000.

Usage

With this command, configure the maximum limit to the pending ATTACH/RAU messages queue in the LinkMgr. When the limit is reached, the LinkMgr sends the Query/Forward messages to the IMSIMgr.
As the IMSIMgr gets busier and does not responded to Query/Forward requests, the response to the requests will get slower and slower and the queue size continues inflating if the incoming message rate is high. To avoid this situation, set the **max-pending-attaches** for the pending queue for Attach and RAU messages. All other messages from the HLR will be added to the queue as they cannot be dropped. High and low watermarks are set to the queue at 80% of **max-pending-attaches** " and 60% of **max-pending-attaches** respectively.
Once a high watermark is reached, the new Attach and RAU requests are dropped and relevant statistics are incremented. Once a low watermark is hit, the new Attach/RAU requests are accepted and added to the pending queue. The entries are added to the pending queue only when the window-size between IMSIMgr and LinkMgr becomes zero. This is a very rare occurrence and will not affect the current behavior in normal circumstances.

Example

Set the queue length to a maximum of *15000* requests:

```
max-pending-attaches 15000
```

old-tlli invalidate tlli

This command configures a list of random TLLI to be invalidated (removed) from the GMM after the invalidate old-TLLI timer expires.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

`[ no ] old-tlli invalidate tlli` *`< hexadecimal >`*

`no`

Removes a single random TLLI from the configured list.

`< hexadecimal >`

Identifies a single random TLLI to be removed from the GMM after the old-TLLI timer expires.

Usage

Use this command to create a list of up to 50 random TLLI to be dropped from the GMM after the old-TLLI timer expires. This command also starts the invalidate old-TLLI timer.

Important: If the old-TLLI expiry timer is not configured with the **`old-tlli hold-time`** command, then the SGSN will only drop second Attach Requests using the same random TLLI already in use.

Related Commands:

- The **`gmm-message`** configures the SGSN to discard (drop) the Attach-Request message received with a random TLLI already in use
- The **`old-tlli hold-time`** command configures the old-TLLI expiry timer.

Example

Add random TLLI *`0x7f05a30a`* to the Invalidate List:

```
old-tlli invalidate tlli 0x7f05a30a
```

old-tlli hold-time

This command configures the old-TLLI expiry timer to be started in GMM when anyone of the listed random TLLI are received.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default ] old-tlli hold-time < seconds >
```

default

Resets the timer to 5 seconds

< seconds >

Sets the numbers of seconds before the timer expires; range 1 to 125.

Usage

Use this command to configure the old-TLLI expiry timer to be started in GMM when anyone of the listed random TLLI are received. If the timer expires prior to receiving Attach-Complete then the SGSN invalidates (removes) the TLLI from the GMM.

Important: For this configuration to work, the list of random TLLI to be removed (invalidated) from the GMM must be defined with the **old-tlli invalidate tlli** command.

Related Commands:

- The **gmm-message** configures the SGSN to discard (drop) the Attach-Request message received with a random TLLI already in use
- The **old-tlli invalidate tlli** command configures the random invalidate TLLI list.

Example

Set the timer for *2* seconds:

```
old-tlli hold-time 2
```

pdp-deactivation-rate

Set the rate the SGSN deactivates PDP connections per second per SessMgr when GPT-C path failure is detected.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
pdp-deactivation-rate { connected-ready rate | idle-standby rate }

default pdp-deactivation-rate { connected-ready | idle-standby }
```

default

If this keyword is used with the command, then the default deactivation rates are used.

connected-ready *rate*

Subscribers that are in the PMM-Connected / GPRS-Ready state and actively using the SGSN service need to be deactivated at a faster rate to facilitate the deactivation/re-activation process.
rate -sets the number of subscribers to be deactivated per second per SessMgr and the valid range is 1 to 1000 and the default is 760 connected-ready subscribers deactivated per second.

idle-standby *rate*

Subscribers that are in the PMM-Idle / GPRS-Standby state are not actively using the SGSN service and can be deactivated at a slower rate. The deactivation process for idle-standby subscribers includes paging before the Deactivate Request is sent.
rate - sets the number of subscribers to be deactivated per second per SessMgr and the valid range is 1 to 1000 and the default is 240 idle-standby subscribers deactivated per second.

Usage

Use this command to define a rate at which the SGSN processes PDP deactivations when a GTP-C path failure is detected (and confirmed according to the SGSN's default behavior). The operator can use this command to set a deactivation rate that ensures radio network congestion is avoided.
Related commands:

- **max-remote-restart-counter-change** - allows the operator to set a maximum variance between stored and received values for restart counter changes coming from the GGSN. For details, refer to the SGSN Global configuration mode documentation.
- **disable-remote-restart-counter-verification** - allows the operator to disable the default behavior. For details, refer to this command in the SGSN Global configuration mode documentation.

Example

Use the following command to deactivate PDP connections for *600* PMM-Connected / GPRS-Ready subscribers per second:

```
pdp-deactivation-rate connected-ready 600
```

Use the following command to deactivate PDP connections for *320* PMM-Idle / GPRS-Standby subscribers per second:

```
pdp-deactivation-rate idle-standby 320
```

Use the following command to reset the default *760* per second deactivation rate for PMM-Connected / GPRS-Ready subscribers:

```
default pdp-deactivation-rate connected-ready
```

ranap excess-len ignore

Configure the SGSN to ignore excess length of received RANAP messages.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] ranap excess-len ignore
```

default

Resets the default behavior - a decode error is generated when received RANAP messages are more than an extra octet in length.

no

Disables the configuration to ignore overly long RANAP messages.

Usage

By default, the SGSN issues a decode error when the RANAP messages include extra octets. Use this command to ignore RANAP messages that have excess octets.

Example

Use the following command to enable the SGSN to ignore overly long RANAP messages:

```
ranap excess-len ignore
```

Use the following command to disable ignoring of RANAP messages that are excessive in length:

```
no ranap excess-len ignore
```

ran-information-management

Enable/disable RAN information management (RIM) support for the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] ran-information-management
```

default

Resets the default so RIM is disabled.

no

Disables the RIM support in the configuration file.

Usage

By default, handling of RAN information management (RIM) messages is disabled. This command enables the SGSN to handle RIM messages. When this command is enabled and RIM message handling is enabled on the destination node, then RIM PDUs will be forwarded to the BSC/RNC. If RIM message handling is not enabled on both nodes, then the RIM PDUs will be dropped silently.
Confirm RIM configuration with the **show sgsn-mode** command in the Exec mode.

Example

Use the following command to enable RIM support:

```
ran-information-management
```

Use the following command to disable RIM support that has been added to the configuration:

```
no ran-information-management
```

target-offloading

Selects the subscriber offloading algorithm to be applied to the SessMgr and the IMSIMgr.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
target-offloading algorithm [ optimized-for-speed | optimized-for-target-count ]

default target-offloading algorithm
```

default

Resets the configuration to default values.

optimized-for-speed

Enables faster algorithm to achieve the target count.

optimized-for-target-count

Enables a reliable algorithm to achieve the target count.
Default.

Usage

With the SGSN's distributed architecture, there are many SessMgrs and offloading will happen in parallel at all SessMgrs. This command enables the operator to control the total number of subscribers being offloaded.

Important: The value for this command can not be altered once dynamic offloading has begun - refer to the command description for the **sgsn-offload** command in the *Exec Mode* chapter..

Example

Set the SGSN to use the faster algorithm for offloading:

```
target-offloading algorithm optimized-for-speed
```

tlli-cb-audit

This command enable (default is disabled) or disables a periodic (hourly) audit of TLLI-CBs in the BSSGP layer.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
tlli-cb-audit

[ default | no ] tlli-cb-audit
```

default

Include **default** with the command to disable the audit function.

no

Include **no** with the command to disable the audit function.

Usage

This command is used to clean-up hanging or unassociated TLLI in the BSSGP layer. This configuration defined with this command will be common to all NSE configured for this SGSN.
Independent of this command configuration, the SGSN triggers and audit when the number of TLLI-CBs reaches 35,000.

Example

Use the following command to enable the hourly audit for unassociated TLLl-CBs:

```
tlli-cb-audit
```

umts-aka-r99

This command enables the operator to authenticate mobile equipment (MEs) with R99+ USIMs and capable of UMTS AKA.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
umts-aka-r99

no umts-aka-r99
```

no

Including **no** with the command disables the authentication.

Usage

This command enables operators to authenticate MEs that are attempting to connect to a 2.5G network with R99+ USIMs if the MEs are UMTS AKA capable. For R99 mobiles, the SGSN will continue to perform GSM AKA even if quintuplets are received fromthe HLR.

Example

Use the following command to disable UMTS AKA authentication for MEs with R99+ USIMs:

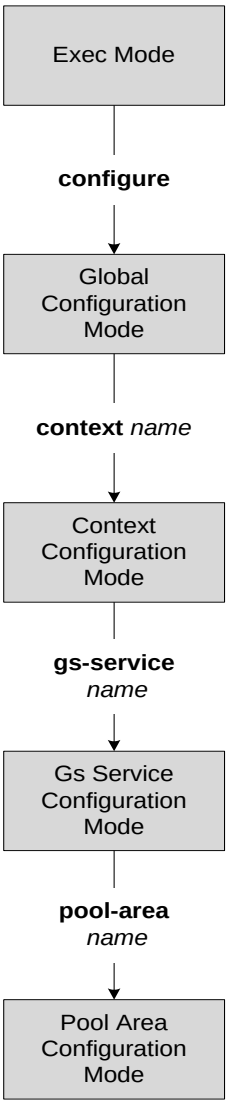
```
no umts-aka-r99
```

Chapter 252
SGSN Pool Area Configuration Mode Commands

The Pool Area configuration mode configures the parameters used to setup the VLRs to use with a pool area in a Gs service.

With this mode, the command prompt will be similar to:

```
[ctx_name]hostname(config-gs-pool-area)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Return to the Exec mode.

exit

Exits the current configuration mode and returns to the previous configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the previous configuration mode.

hash-value

This command configures the load distribution for the VLRs that service this pool area.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

hash-value { *hash_value* | non-configured-values | range *start_value* to *end_value* } use-vlr *vlr_name*

no hash-value { *hash_value* | non-configured-values | range *start_value* to *end_value* }

no

Removes the configured Gs procedures from this Gs service.

hash_value

Specifies the specific hash value for VLR(s).
hash_value must be an integer value from 0 through 999.

range *start_value* **to** *end_value*

Specifies the range of hash values for a VLR.
start_value specifies the start value for range of hash and is an integer value from 0 through 999.
start_value must be lower than *end_value.*
end_value specifies the end value for range of hash and is an integer value from 0 through 999. *end_value* must be higher than *start_value*.

non-configured-values

This keyword assign all non-configured hash values to use the named VLR.

use-vlr *vlr_name*

Specifies the name of the VLR to be associated with this pool area.
vlr_name is the name of VLR and must be an alpha and/or numeric string of 1 to 63 characters.

Usage

Use this command to command configures the load distribution for the VLRs that service this pool area as defined in TS 23.236.
The algorithm for selection of VLR from a pool area is based on the hash value computed on the IMSI digits. The SGSN derives a hash value (V) using procedure as defined in TS 23.236. Every hash value from the range 0 to 999 corresponds to a single MSC/VLR node. Typically many hash values may point to the same MSC/VLR node.
This command can be entered multiple times for different hash value.

Example

Following command configure the all non configured hash values to use VLR named *starvlr1* in this pool area:

hash-value non-configured-values use-vlr *starvlr1*

lac

This command defines a set of location area code (LAC) values for a pool area.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

lac *lac_id* **+**

no lac *lac_id*

no

Removes the configured LAC value from this pool area configuration.

lac *lac_id*

Specifies the subscribers' location area code (LAC) to be associated with this pool area and a specific VLR. This LAC is obtained from the radio area identity (RAI).
lac_id: Must be an integer from 1 through 65535.

+

More than one *lac_id*, separated by a space, can be entered within a single command.

Usage

Use this command to specify a set of LACs to use for a pool area.
This command can be entered multiple times, subject to a limit of 32 LAC definitions (total for **non-pool-area** and **pool-area** configuration) per Gs service.

Important: LAC values across multiple pool areas and non-pool-areas must be unique within the Gs service.

Example

The following command configures LACs *101, 301,* and *222* for the pool area.

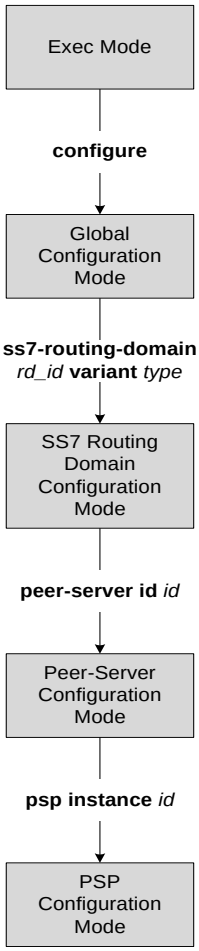
```
lac 101 301 222
```

Chapter 253
SGSN PSP Configuration Mode Commands

The Peer-Server Process (PSP) configuration mode provides the commands to create, configure, bind, and manage a specific PSP instance included in an SS7 routing domain configuration.

In this mode, where information in italics is customer-defined, the command prompt should appear similar to:

```
[local]hostname(config-ss7-rd-1-ps-1-psp-1)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

associate

Defines an association between the PSP instance and an application server process (ASP) instance.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
associate asp instance asp_num

no associate
```

no

Removes the association between the PSP and the ASP from the routing domain configuration.

Important: Using the **no associate** command will probably result in the termination of all current subscriber sessions active through the peer-server.

asp_num

Identifies a specific ASP configuration. Up to four ASP instances can be configured for a single SS7 routing domain.
asp_num must be an integer from 1 through 4.

Usage

Use this command to create an association between a specific peer-server process (PSP) and a specific application server process (ASP) instance.
Before using the **associate** command, the values for the **psp-mode** and **end-point** commands must be configured.
Before using the **associate** command, the M3UA end-point of the ASP must be configured. Use the commands defined in the *ASP Configuration Mode* chapter of the *Command Line Interface Reference*.

Example

Associate this PSP instance with an ASP configuration instance:

```
associate asp instance 2
```

end

Exits the configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Change the mode back to the Exec mode.

end-point

This command defines or deletes the IP address to be associated with the local SCTP end-point for the application server process (ASP).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end-point { address ip_address | port port_number }

no end-point [ address ip_address ]
```

port *port_number*

Configures the M3UA's SCTP port number for the end-point.
port_number: Must be an integer from 1 to 65535.
Default: 2905.

no

Removes the ASP end-point association configuration from the PSP configuration.

Important: This command can not be used as long as the PSP and the ASP are associated. Use the **no associate** command when entering any form of this command, including **no end-point**. When the change is made, re-enter the ASP association with the **association** command.

Usage

Use this command to manage the ASP end-point. At least one address needs to be configured for the ASP before the end-point can be associated with the PSP.

Example

Set the ASP end-point to IP address 192.168.1.1 with the following command:

```
end-point address 192.168.1.1
```

exchange-mode

Configures the exchange-mode for the PSP communication.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exchange-mode [ double-ended | single-ended ]
```

Usage

Important: Before using this command to set a value or reset the default, you must disassociate the PSP instance with the **no associate** command. When you have modified your configuratioin with this command, then use the **associate** command to setup a new ASP association.

Use this command to toggle the exchange modes for the PSP to match the exchange mode supported by the ASP. The exchange mode specifies what type of ASP messages exchange is used in an IPSP communication. The **exchange-mode** must be configured for 'single-ended' if the **psp-mode** has been configured for 'client'.

Example

Change the exchange mode from the standard double-ended to single-ended:

```
exchange-mode single-ended
```

exit

Exits the current configuration mode and moves to the previous configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the Peer-Service configuration mode.

psp-mode

Configures either client-mode or server-mode as the PSP's operational mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
psp-mode { client | server }
```

client

The PSP operates as a client.

server

The PSP operates as a server.

Usage

Important: Before using this command to change the configuration, you must disassociate the PSP instance with the **no associate** command. When you have modified your configuratioin with this command, then use the **associate** command to setup a new ASP association.

Example

Instruct the peer-server process to operate in either client or server mode.

Configure the PSP to operate in server mode:

```
psp-mode server
```

routing-context

Configures the behavior of the routing context in M3UA messages.

Important: This keyword function is only available in releases 8.1 and higher.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
routing-context { discard-inbound | process-inbound { insert-outbound | suppress-outbound
}
```

```
default routing-context
```

default

Include this keyword with the command, to reset the configuration to the system default for routing-context which is a combination of process-inbound and insert-outbound.

discard-inbound

Sets the routing context received in M3UA messages to be discarded.

process-inbound

Sets the routing context received in M3UA messages to be processed.

insert-outbound

Sets the routing context so that it is added in the M3UA messages.

suppress-outbound

Sets the routing context so that it is suppressed in the M3UA messages.

Usage

Important: Before using this command to change the configuration or reset the default, you must disassociate the PSP instance with the **no associate** command. When you have modified your configuratioin with this command, then use the **associate** command to setup a new ASP association.

In PSP (singled-ended) configuration mode, the settings for both the local routing context (the SGSN's routing context) and the peer routing context (the RNC's routing context) should be the same. If the routing contexts created at the SGSN and on the peer are different then this can cause the M3UA link to fail. Routing context is an optional parameter when an M3UA association has only one associated peer-server.

Example

If the peer does not support routing context, then disable the routing context feature:

```
routing-context discard-inbound suppress-outbound
```

sctp-alpha

This stream control transmission protocol (SCTP) retransmission time out (RTO) parameter defines the RTO-Alpha value.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sctp-alpha *value*

default sctp-alpha

value

Defines a percentage (%) that represents the RTO portion of the round-trip time (RTT) calculation. This percentage value must be an integer between 0 and 65535.

default

Resets the **sctp-alpha** to the default value of 5%.

Usage

sctp-alpha is used in conjunction with other commands, such as the **sctp-beta** command, to determine the round-trip time (RTT) calculations. The Alpha parameter is used to manage load balancing within the SS7 environment for multi-homed peers.

Important: Before using this command to set a value or reset the default, you must disassociate the PSP instance with the **no associate** command. When you have modified your configuratioin with this command, then use the **associate** command to setup a new ASP association.

Example

Set the SCTP RTO-Alpha value to 256% of the RTT calculation:

sctp-alpha *256*

sctp-beta

This stream control transmission protocol (SCTP) retransmission time out (RTO) parameter defines the RTO-Beta value.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sctp-beta *value*

default sctp-beta

value

Defines a percentage (%) that represents the RTO portion of the round-trip time (RTT) calculation. This percentage value must be an integer between 0 and 65535.

default

Resets the **sctp-beta** to the default value of 10%.

Usage

Use this command in conjunction with other commands, such as the **sctp-alpha** command, to determine the round-trip time (RTT) calculations. The Beta parameter is used to manage load balancing within the SS7 environment for multi-homed peers.

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Example

Set the SCTP RTO-Alpha value to 512% of the RTT calculation:

sctp-beta *512*

sctp-checksum-type

This command selects the type of checksum algorithm to be used.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
sctp-checksum-type { adler32 | crc32 }

default sctp-checksum-type
```

adler32

Selects the Adler-32 type of algorithm as a faster checksum function.

crc32

Selects the CRC-32, a slower but more reliable 32-bit cyclic redundancy check.

default

Resets the **sctp-checksum-type** to the default of CRC-32.

Usage

Use this command to set which type of checksum algorithm the SGSN is to use to validate SCTP packets.

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Example

```
sctp-checksum-type crc32
```

sctp-cookie-life

This command sets the SCTP valid cookie life.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sctp-cookie-life *value*

default sctp-cookie-life

value

Sets the valid cookie life value in increments of 100 milliseconds. The range is 50 to 1200 .

default

Resets the **sctp-cookie-life** value to the default, 600 (= .6 seconds).

Usage

Use this command to set the SCTP cookie life.

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Example

Set the SCTP cookie life to 1 second (1000 milliseconds):

sctp-cookie-life *1000*

sctp-init-rwnd

This command sets the size of the SCTP receiver window .

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sctp-init-rwnd *window_size*

default sctp-init-rwnd

window_size

Sets an integer to configure the window size. The range is 32768 to 1048576.

default

Resets the **sctp-init-rwnd** window size to the default, 1048576.

Usage

Use this command to set the receiver window size in the configuration. Configuring this parameter enables the SCTP client to send configured 'sctp-init_rwnd' as a_rwnd parameter in the INIT message. For the SCTP server, the INIT ACK will be populated with sctp-init_rwnd as a_rwnd parameter per RFC 4960.
The command enables the operator to configure a reduced priority for LinkManager Control messages, thereby giving Timer messages the highest priority. The Timer messages are retained at the highest priority and Data messages are kept at a lower priority.

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Example

Use the following command to set the SCTP window size to 32786:

sctp-init-rwnd *32768*

sctp-max-assoc-retx

This command sets the maximum number of datagram retransmissions to be associated with this peer server configuration.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sctp-max-assoc-retx *value*

default sctp-max-assoc-retx

value

Defines the maximum number of datagram retransmissions for an association. The value must be an integer between 0 and 255.

default

Resets the default for **sctp-max-assoc-retx** to 10.

Usage

Use this command to configure the maximum number of datagram retransmissions for an association. The endpoint will be declared unreachable after **sctp-max-assoc-retx** number of consecutive retransmissions to an endpoint on any transport address.

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Example

sctp-max-assoc-retx *3*

sctp-max-init-retx

This command sets the maximum number of retries to send the INIT datagram.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sctp-max-init-retx *value*

default sctp-max-init-retx

value

Sets the maximum number of retries. This value must be an integer between 0 and 255.

default

Resets the default for **sctp-max-init-retx** to 5.

Usage

Use this command to set the maximum number of retries the SCTP layer should make to send the INIT datagram to the peer to open an association.

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Example

sctp-max-init-retx *3*

sctp-max-mtu size

This command sets the number of bytes that comprise the maximum MTU size.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sctp-max-mtu-size *value*

default sctp-max-mtu-size

value

Sets the maximum number of bytes for the SCTP MTU size. This value must be an integer between 508 and 65535.

default

Resets the default for **sctp-max-mtu-size** to 1500 bytes.

Usage

Use this command to configure the size of the MTU.

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Example

Set the maximum size of the MTU to 3000 bytes:

sctp-max-mtu-size *3000*

sctp-max-out-strms

This command sets the maximum number of outgoing streams through the PSP going towards the peer server.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sctp-max-out-strms *max#_out_streams*

default sctp-max-out-strms

default

Resets the SGSN's **sctp-max-out-strms** value to the default of 16.

max#_out_streams

The value must be an integer between 1and 65535. The value should match the peer node's (STP/SG/RNC/HLR) number of in-bound streams.

Usage

Use this command to balance the stream throughput from the PSP to the peer server. The value for this command is used to validate the incoming packets in the SCTP layer.

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Example

sctp-max-out-strms *3500*

sctp-max-path-retx

This command sets the maximum number of datagram retransmissions for this path.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sctp-max-path-retx *value*

default sctp-max-path-retx

value

Sets the maximum number of datagram retransmission to a destination transport address. This value must be an integer from 0 to 255.

default

Resets the **sctp-max-path-retx** default to 5.

Usage

Use this command to set the maximum number of datagram retransmissions to a destination transport address. The destination transport address will be declared unreachable after the SGSN exhausts the **sctp-max-path-retx** number of consecutive retransmissions to a destination transport address.
Depending upon network conditions, lower values typically means faster detection of SCTP-Path failure.

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Example

sctp-max-path-retx *10*

sctp-rto-initial

This command sets the initial retransmission timeout for the SCTP.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sctp-rto-initial *value*

default sctp-rto-initial

default

Resets the system to the **sctp-rto-initial** default of 30 (3 seconds).

value

The value must be an integer between 1 and 50.

Usage

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Use this command to define the initial retransmission timer.
The value set for **sctp-rto-initial** should be greater than or equal to the minimum value set with **sctp-rto-min** (**sctp-rto-initial**=> **sctp-rto-min**).
The value set for **sctp-rto-initial** should be less than or equal to the maximum value set with **sctp-rto-max** (**sctp-rto-initial** <= **sctp-rto-max**).

Example

sctp-rto-initial *240*

sctp-rto-max

This command sets the maximum retransmission timeout value for the SCTP.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sctp-rto-max *value*

default sctp-rto-max

default

Resets the system to the **sctp-rto-max** default of 600 (60 seconds).

value

Set the maximum retransmission timeout value in increments of 100 milliseconds (0.1 seconds) and the value must be an integer between 5 and 1200.

Usage

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Use this command to configure the maximum time for retransmissions.
The value set for **sctp-rto-max** should be greater than or equal to the value set for **sctp-rto-initial** (**sctp-rto-max** => **sctp-rto-initial**).

Example

The following sets the timeout for 45 seconds:

sctp-rto-max *450*

sctp-rto-min

This command sets the minimum retransmission timeout (RTO) value for the SCTP.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sctp-rto-min [units-10ms] *value*

default sctp-rto-min

default

Resets the **sctp-rto-min** to the default of 10 (1 second).

units-10ms

Including this keyword, before entering a value, enables configuration with finer granuality - in 10 millisecond units.

value

If the **units-10ms** keyword is included, then set the timeout in increments of 10 milliseonds. The value must be an integer between 1 and 500.
If the **units-10ms** keyword is not included then set the timeout in increments of 100 milliseconds. The value must be an integer between 1 and 50.

Usage

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Use this command to set the minimum time for retransmission before timeout.
The value set for **sctp-rto-min** should be less than or equal to the value set for **sctp-rto-initial** (**sctp-rto-min** <= **sctp-rto-initial**)

Example

The following sets the timeout for 2 seconds:

```
sctp-rto-min 20
```

sctp-sack-frequency

This command sets the frequency of transmission of SCTP selective acknowledgements (SACK).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sctp-sack-frequency [units-10ms] *value*

default sack-frequency

value

Sets the maximum number of datagrams to be received prior to sending a SACK to the peer. The value must be an integer between 1 and 5.

default

Resets the **sctp-sack-frequency** default value of 2.

Usage

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Use this command to set the maximum number of datagrams to be received before a SACK must be sent to the peer. The **sctp-sack-frequency** is used in conjunction with the **sctp-sack-period** to control the generation of SACK, depending on which one occurs first.

Example

sctp-sack-frequency *3*

sctp-sack-period

This command sets the delay before sending an SCTP selective acknowledgement (SACK).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sctp-sack-period [units-10ms] *value*

default sack-period

units-10ms

Including this keyword, before entering a value, enables configuration with finer granuality - in 10 millisecond units.

value

If the **units-10ms** keyword is included, then set the timeout in increments of 10 milliseonds. The value must be an integer between 0 and 50.
If the **units-10ms** keyword is not included then set the timeout in increments of 100 milliseconds. The value must be an integer between 0 and 5.

default

Resets the system to the **sctp-sack-period** default value, 2 (=200 milliseconds).

Usage

Use this command to set the time the SCTP waits to send a SACK.

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Example

sctp-sack-period *3*

sctp-suppress-alarm

This command enables/disables the suppression of alarms for SCTP path failure between two peer endpoints.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] sctp-suppress-alarm path-failure self-end-point-address *orig_ipv4_address***peer-end-point-address** *peer_ipv4_address*

no

Disables the pre-configured alarm suppression for SCTP path failure.

path-failure

This keyword specifies that the alarm suppression is for SCTP path failure between two peer nodes.

self-end-point-address *orig_ipv4_address*

This keyword specifies the IP address of the originating endpoint.
orig_ipv4_address is the IP address of originating endpoint in IPv4 dotted decimal notation.

peer-end-point-address *peer_ipv4_address*

This keyword specifies the IP address of the peer endpoint.
peer_ipv4_address is the IP address of peer endpoint in IPv4 dotted decimal notation.

Usage

Use this command to configure the path failure alarm suppression. This command ignores the alarms generated on SCTP path failure.

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Example

The following command suppresses the path failure alarms occurred in SCTP path between originating peer address *1.2.3.4* and peer endpoint *6.7.8.9*:

sctp-suppress-alarm path-failure self-end-point-address *1.2.3.4* **peer-end-point-address** *6.7.8.9*

timeout

This command sets the times for various timeout timers.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

timeout {**m3ua-periodic-dest-audit** *dest_timeout* | **sctp-bundle** *bundle_time* | **sctp-heart-beat** *hrt_bt_timeout*}

default timeout sctp-heart-beat

default

Resets the system to the default value for the SCTP heartbeat interval.

m3ua-periodic-dest-audit *dest_timeout*

Sets the period (in increments of seconds) between the DAUD messages while auditing a destination state.
dest_timeout: Must be an integer from 1 to 65535. Default is 2.

sctp-bundle *bundle_time*

Enables SCTP bundling and sets the SCTP bundle timeout value in incremenets of 100 milliseconds. SCTP bundling provides better bandwidth utilization and less traffic, however, there is a 100 millisecond packet transmission delay.

Important: Peer end should also be configured to support SCTP bundling.

Default: SCTP bundling is disabled.
bundle_time : Enter an integer from 1 to 65535.

sctp-heart-beat *hrt_bt_timeout*

Sets the number of seconds in the SCTP heart-beat timer
hrt_bt_timeout: This value is an integer between 1 and 300. Default is 30.

Usage

Use this command to configure timers. Repeat the command with each of the keywords to set values for each.

Important: Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Example

timeout m3ua-periodic-dest-audit *120*

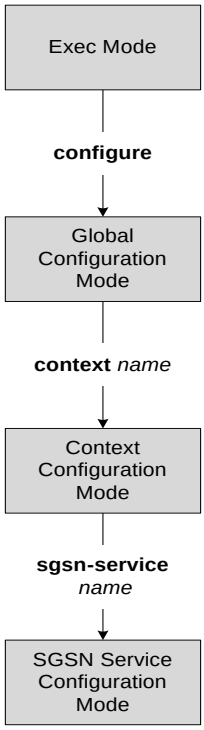
Chapter 254
SGSN Service Configuration Mode Commands

The SGSN Service configuration mode is used within the global configuration mode to specify the 3G operations of the SGSN and the available SGSN services for a specific context.

SGSN Service works with MAP Service, SGTP Service, GTPP Group, and IuPS Service. All five of these services must be configured to enable a 3G SGSN to communicate with other elements within a UMTS network.

In this mode, the command prompt should appear like:

```
[<ctx_name>]hostname(config-sgsn-service)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

accounting

This command defines the accounting context name and enables/disables specific types of CDR generation for the accounting in the SGSN service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

accounting (cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr } } + | context *cntx_name* **}**

default accounting cdr-types

no accounting (cdr-types | context }

default

Returns the system to default settings for the selected type of CDR.

no

Removes the pre-configured type of CDR generation for accounting from the SGSN service.

cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr } +

Default: enabled
Defines the types of CDRs to be generate:d within the specified SGSN service for accounting:

- **mcdr** Enables generation of M-CDRs.
- **scdr** : Enables generation of S-CDRs.
- **sms** : Enables generation of SMS-type CDRs based on one of the following:
- **mo-cd:** : SMS CDRs orignates from the mobile.
- **mt-cdr:** SMS CDRs terminates at the mobile.

+

Specifies that the specified keywords with in the group can be entered multiple times with a single command.

context *cntx_name*

Specifies an accounting context to be associated with the SGSN service.
cntx_name: Define a string of 1 to 79 alphanumeric characters.

Usage

Use this command to define the type of CDRs to generate for SGSN service. By default all type of CDRs are generated. Note that change of this configuration will be applied to new call and/or to new PDP contexts only.
By default, generation of the S-CDR, M-CDR, SMS-MT-CDR, and SMS MO-CDR types is enabled.

Example

The following command configures the system to generate CDRs of M-CDR type for accounting in the current SGSN service:

accounting cdr-types *mcdr*

admin-disconnect-behavior

This command defines some of the actions the SGSN will take during an Admin-Disconnect procedure.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
admin-disconnect-behavior { clear-subscription | detach-type { reattach-not-required |
reattach-required } }

[ default | no ] admin-disconnect-behavior { clear-subscription | detach-type }
```

clear-subscription

Including this keyword in the configuration instructs the SGSN to clear subscriber contexts and the subscription data database whenever the **clear subscribers all** command is issued (from the Exec mode) for attached subscribers. As well, the SGSN will issue an appropriate Map-Purge-MS-Req to the HLR if needed.
Default: disabled

detach-type

Including this keyword defines which type of detach instruction to include in the Detach-Request message during an Admin-Disconnect procedure. One of the following options must be included when this command is entered:

- **reattach-not-required**
- **reattach-required**

Default: reattach-required

default | no

Including either **default** or **no** keyword in the command, instructs the SGSN to use the default value for the specified parameter.

Usage

Include the **clear-subscription** keyword with this command configuration to ensure that more than attached MM-context and active PDP-contexts are cleared when the clear **subscribers all** command is issued for attached subscribers.
To clear subscription data for detached subscribers, refer to the **sgsn clear-detached-subscriptions** command described in the *Exec* mode chapter.
Including the **detach-type** keyword with this command instructs the SGSN to include either a 'reattach-required' or a 'reattach-no-required' instruction in the Detach-Request message.

Example

Configure the SGSN to clear data such as PTMSI allocated, auth-vectors received, and NGAF flag values stored in the subscriber database for attached subscribers:

```
admin-disconnect-behavior clear-subscription
```

cc profile

Configures the charging characteristic (CC) profile with the triggers for generating various types of CDR as defined with the **accounting** command.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

cc profile *profile_bits* **[buckets** *number* **| interval** *time* **| tariff time1** *mins hours* **[time2** *mins hours* **] [time3** *mins hours* **] [time4** *mins hours* **] | volume { downlink** *down_vol* **uplink** *up_vol* **| total** *total_vol* **}] +**

[no | default] cc profile *profile_bits* **[buckets | interval | tariff | volumne]**

no

Removes a previously configured CC profile.

default

Returns the specified CC profile to the original default system settings.

profile_bits

Defines the value of the profile bits for the SGSN service.
index can be configured to any integer value from 0 to 15. Some of the values have been predefined according to 3GPP standard:

- 1 for hot billing
- 2 for flat billing
- 4 for prepaid billing
- 8 for normal billing

buckets *number*

Specifies the number of statistics container changes in the CDR due to QoS changes or tariff times that can occur before an accounting record (CDR) is closed
Default: 4
number : Must be integer from 1 to 4.

interval *time*

Specifies the normal time duration (in seconds) that must elapse before closing an accounting record (CDR) provided that any or all of the following conditions occur:
time : Enter any integer from 60 to 40000000.

tariff time1 *mins hours* **[time2** *mins hours* **time3** *mins hours* **time4** *mins hours* **]**

Specifies the time-of-day (based on a 24-hour clock) to close the current statistics container in the CDR, but not necessarily the CDR itself. One tariff time must be defined and up to four tariff times can be specified.

Important: The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

- *mins*: The minutes of the hour. Enter an integer from 0 to 59.
- *hours*: The hour of the day. Enter an integer from 0 to 23.

volume { downlink *down_vol* **uplink** *up_vol* **| total** *total_vol* **}**

Specifies the downlink, uplink, and total volumes octet counts that must be met for the closure of the CDR.
down_vol : Enter any integer from 100000 to 1345294336.
up_vol : Enter any integer from 100000 to 400000000.
total_vol : Enter any integer from 100000 to 400000000.

Usage

Charging characteristics consist of a profile index and behavior settings. This command configures the profile index for the SGSN's charging characteristics. The SGSN supports up to 16 profile indexes.

Example

The following command configures a profile index of 10 with tariff times of 7:00 AM and 7:30 PM:

```
cc profile 10  tariff time1 0 7 time2 30 19 time3 0 7 time4 30 19
```

check-imei

This command configures the action the SGSN will take if the route towards the EIR is down.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
check-imei { gf-failure-action | gf-timeout-action } { continue | reject }

default check-imei { gf-failure-action | gf-timeout-action }
```

default

Resets the default function to reject the Attach.

gf-failure-action

Coupled with either **continue** or **reject**, this keyword instructs the SGSN to take action if a valid EIR configuration exists under the MAP service and if the EIR is temporarily unreachable due to associated DPC/SSN inaccessible/out-of-service.

gf-timeout-action

Coupled with either **continue** or **reject**, this keyword instructs the SGSN to take action if a valid EIR configuration exists under the MAP service and the route to the EIR is available, but no response is received from the EIR.

continue

Instructs the SGSN to continue the Attach process.

reject

Instructs the SGSN to reject the Attach process.

Usage

Typically, the Attach process will be continued when there is an IMEI check timeout based on the configuration under the SGSN service configuration and/or the GPRS service configuration. But this works only if the route towards the EIR is UP and the IMEI request timer expires. This command configures the SGSN to allow the Attach process to continue in the case the route towards the EIR is down, that is the DPC / SSN is out-of-service.

Example

Use the following command to reset the default and reject Attach:

```
default check-imei gf-failure-action
```

check-imei-timeout-action

In Releases 12.0 and higher, this command has been replaced with enhanced functionality in the **check-imei** command, also available in this configuration mode.

core-network

This command specifies the numeric ID for a core network to identify which CN is to be used by the SGSN service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
core-network id cn_id

no core-network id
```

no

Removes the currently configured core network ID from the current SGSN configuration.

id *cn_id*

This number identifies the core network to connect the SGSN service.
cn_id : Must be an integer from 0 through 65535.

Usage

Use this command to set a global ID to identify this SGSN in the core network.

Example

The following command sets the core network ID for the current SGSN service to 127:

```
core-network id 127
```

disable/enable super-charger

This command has been deprecated and replaced by the **super-charger** command. For the commands to configure the SuperCharger feature, refer to the *Call-Control Profile Configuration Mode* chapter.

dns israu-mcc-mnc-encoding

Configures either decimal or hexadecimal format for the MCC and MNC values in the DNS query which is sent during the ISRAU.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
dns israu-mcc-mnc-encoding { decimal | hexidecimal }

default dns israu-mcc-mnc-encoding
```

default

Resets the SGSN to send the MCC and MNC values in decimal format for DNS queries.

decimal

Default.
Instructs the SGSN to send the MCC and MNC in decimal format in the DNS query.

hexadecimal

Instructs the SGSN to send the MCC and MNC in hexadecimal format in the DNS query.

Usage

Use this command to determine the type of encoding for the MCC and MNC to be included in the DNS query sent during the inter-SGSN RAU (ISRAU). The choice must match the format of the DNS server. For example:
In decimal, the MNC/MCC in a DNS query would appear like:

```
rac0017.lac42e3.mnc310.mcc722.gprs
```

In hexadecimal, the MNC/MCC in a DNS query would appear like:

```
rac0017.lac42e3.mnc0136.mcc02d2.gprs
```

Example

Use hexadecimal values for the MCC/MNC in the DNS query.

```
dns israu-mcc-mnc-encoding hexadecimal
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Return to the Exec mode.

exit

Exits the current configuration mode and returns to the context configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the context configuration mode.

gmm

This command defines the GPRS mobility management parameters for the SGSN service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gmm { T3302-timeout *t3302_dur* **| T3312-timeout** *t3312_dur* **| T3313-timeout initial** *t3313_init* **[decrease** *t3313_decrement* **| increase** *t3313_increment* **]** | **T3322-timeout** *t3322_dur* **| T3350-timeout** *t3350_dur* **| T3360-timeout** *t3360_dur* **| T3370-timeout** *t3370_dur* **| implicit-detach-timeout** *impli_detach_dur* **| max-auth-retransmission** *auth_retrans* **| max-identity-retransmission** *id_retrans* **| max-page-retransmission** *page_retrans* **| max-ptmsi-reloc-retransmission** *ptmsi_reloc_retrans* **| mobile-reachable-timeout** *ms_reach_dur* **| perform-identity-on-auth-failure | purge-timeout** *purge_dur* **| trau-timeout** *trau_dur* **}**

default gmm { T3302-timeout | T3312-timeout | T3313-timeout | T3322-timeout | T3350-timeout | T3360-timeout | T3370-timeout | implicit-detach-timeout | max-auth-retransmission |max-identity-retransmission | max-page-retransmission | max-ptmsi-reloc-retransmission | mobile-reachable-timeout | perform-identity-on-auth-failure | purge-timeout | trau-timeout }

no gmm { implicit-detach-timeout | max-auth-retransmission | max-identity-retransmission | perform-identity-on-auth-failure }

default

Sets the default value for the specified parameter.

T3302-timeout *t3302_dur*

Default: 10
Specifies the retransmission timer value to guard the GPRS attach or RAU procedure on MS side. *t3302_dur* is the waiting duration in minutes before retransmitting the specific message and must be an integer from 1 through 186.

T3312-timeout *t3312_dur*

Default: 54
Specifies the retransmission timer value to guard the RAU procedure initiation on network side. *t3312_dur* is the waiting duration in minutes before retransmitting the specific message and must be an integer from 1 through 186.

T3313-timeout initial *t3313_init* **[decrease** *t3313_decrement* **| increase** *t3313_increment* **]**

Default: 5
Specifies the retransmission timer value to guard the for paging request procedure initiation on network side.
initial *t3313_init* - Specifies the initial wating duration in seconds before retransmitting the specific message. *t3313_init* must be an integer from 1 through 60.

decrease *t3313_decrement* - Specifies the decrement of the initial timer value in seconds. *t3313_decrement* must be an integer from 1 through 5.
increase *t3313_increment* - Specifies the increment of the initial timer value in seconds. *t3313_decrement* must be an integer from 1 through 5.

T3322-timeout *t3322_dur*

Default: 6
Specifies the retransmission timer value to guard the GPRS detach request procedure on network side. *t3322_dur* is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.

T3350-timeout *t3350_dur*

Default: 6
Specifies the retransmission timer value to guard the GPRS attach accept/RAU accept/realloc request procedure sent with P-TMSI and/or TMSI on network side.
t3350_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.

T3360-timeout *t3360_dur*

Default: 6
Specifies the retransmission timer value to guard the authentication and cipher request procedure on network side.
t3360_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.

T3370-timeout *t3370_dur*

Default: 6
Specifies the retransmission timer value to guard the identity request procedure on network side.
t3370_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.

---

implicit-detach-timeout *impli_detach_dur*

Default: 3600
Specifies the retransmission timer value to guard the implicit detach procedure on network side.
impli_detach_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 3600.

---

max-auth-retransmission *auth_retrans*

Default: 4
Specifies the maximum retransmission of authentication requests allowed.
auth_retrans is the number of retries before declaring the authentication failure and must be an integer from 1 through 10.

---

max-identity-retransmission *id_retrans*

Default: 4
Specifies the maximum retransmission of identity requests allowed.
id_retrans is the number of retries before declaring the identity failure and must be an integer from 1 through 10.

max-page-retransmission *page_retrans*

Default: 5
Specifies the maximum retransmission of page requests allowed.
id_retrans is the number of retries before declaring the paging request failure and must be an integer from 1 through 5.

max-ptmsi-reloc-retransmission *ptmsi_reloc_retrans*

Default: 5
Specifies the maximum retransmission for P-TMSI relocation procedure allowed.
id_retrans is the number of retries before declaring the P-TMSI relocation procedure failure and must be an integer from 1 through 10.

mobile-reachable-timeout *ms_reach_dur*

Default: 58
Specifies the retransmission timer value to guard the mobile reachability procedure on network side.
impli_detach_dur is the waiting duration in minutes before retransmitting the specific message and must be an integer from 4 through 1440.

perform-identity-on-auth-failure

Default: Enabled
Configures the SGSN service to perform an identity check to ascertain the IMSI after an authentication failure on a PTMSI-based message.

purge-timeout *purge_dur*

Default: 10080 (7 days)
Specifies the timer value to guard the detach of MM context procedure on network side.
impli_detach_dur is the waiting duration in minutes before retransmitting the specific message and must be an integer from 1 through 20160.
Define the purge timer to hold detached mm-contexts. Default is 10080 mins (7 days).

trau-timeout *trau_dur*

This timer is available in releases 9.0 and higher.
Default: 30
Specifies the number of seconds the “old” 3G SGSN waits to purge the MS’s data. This timer is started by the “old” SGSN after completion of the inter-SGSN RAU.
trau_dur : Must be an integer from 5 to 60.

Usage

Repeat this command as needed to configure multiple parameters for GPRS mobility management in a UMTS network. This command provides the configuration of timers for mobility procedures and retries for different messages. GMM layer is defined in the 3GPP TS 24.008 (Release 7).

Example

Following command configures the timer to wait for *5* mins before retransmitting the message for GPRS attach or RAU procedure on MS side with maximum number of retries as *6* for authentication:

```
gmm T3302-timeout 5 max-auth-retransmission 6
```

gs-service

This command associates a previously defined Gs service interface to MSC/VLR along with its associated context with an SGSN service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gs-service *gs_srvc_name* **context** *ctx_name*

no gs-service *gs_srvc_name*

no

Removes/disassociates the named Gs service from this SGSN service.

gs_srvc_name

Specifies the name of a specific Gs service for which to display information.
svc_name is the name of a configured Gs service and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

context *ctx_name*

Specifies the specific context name where Gs service is configured. If this keywork is omitted, the named Gs service must be exist in the same context as the SGSN service.
ctx_name is name of the configured context of Gs service. This can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

Usage

Use this command to associate a specific Gs service interface with this SGSN service instance.

Important: A single Gs service can be used with multiple SGSN and/or GPRS service.

Example

Following command associates a Gs service instance named *stargs1*, which is configured in context named *star_ctx*, with an SGSN service:

```
gs-service stargs1 context star_ctx
```

lac

This command defines the location area code (LAC) in hexadecimal format.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

lac *hex*

no lac

no

Erases the **lac** configuration statement.

hex

Enter a hexadecimal number between 0x0 and 0xFFFF

max-pdp-contexts

Configures the maximum number of PDP contexts for a MS (mobile station) that will be supported on this SGSN service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

max-pdp-contexts per-ms *number*

default max-pdp-contexts per-ms

default

Resets the maximum number of PDP contexts per mobile station to the default of 11 for the Gs service configuration

per-ms *number*

Default: 11
Defines the combined total number of primary and secondary PDP contexts for the SGSN service.
number can be an integer from 2 to 11.

Usage

The following example defines 5 as the maximum number of primary and secondary PDP contexts that this SGSN will support for any connected MS.

Example

max-pdp-contexts per-ms *5*

mobile-application-part

This command identifies an already defined MAP service (Mobile Application Part service) to associate with the SGSN service. Although the MAP service does not need to be defined in the same context as the SGSN service, there is a one-to-one relationship between a MAP service and an SGSN service.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mobile-application-part service *map_srvc* **[context** *ctx_name*]

no mobile-application-part service

no

Remove the MAP service association from the SGSN service configuration.

service *map_srvc*

Specifies the name of the MAP service to be associated with this SGSN service.
map_srvc must be the name of a MAP service previously configured on the system.

context *ctx_name*

Specifies the name of the context where the MAP service is configured. If the MAP service is not configured in the current context, then the context where it is configured must be specified to enable the SGSN to reach the MAP service.
If this keyword is not specified, the current context is used.
ctxt_name: Must be the name of the context where the specified MAP service is configured.

Usage

Use this command to identify the MAP service configuration to be used by the SGSN service configuration. Also use this command to specify the context in which the MAP service configuration was created.
If the MAP service is not identified or if the correct context is not identified, then the SGSN service will not START.

Example

The following command specifies a MAP service named map1 that is configured in the same context as the current SGSN service:

```
mobile-application-part service map1
```

network-sharing cs-ps-coordination

Enables/disables the SGSN service to perform a CS-PS coordination check.

Important: This command is no longer available in all 12.0 and 12.2 releases. If you do not see this command in your release, look for the **network-sharing cs-ps-coordination** command in the IuPS Service configuration mode to accomplish the same task. Configuring in the IuPS Service configuration mode allows for the possibility of multiple IuPS services with network-sharing and differing CS-PS coordination requirements.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
network-sharing cs-ps-coordination

default network-sharing cs-ps-coordination

no network-sharing cs-ps-coordination
```

default

Including this keyword resets the SGSN service to allow the check to be performed.

no

Disables this feature for the SGSN service.

Usage

Use this command to facilitate the network sharing functionality. With this command, the SGSN can be instructed to perform a check to determine if CS-PS coordination is needed.
3GPP TS 25.231 section 4.2.5 describes the functionality of the SGSN to handle CS-PS (circuit-switching/packet-switching) coordination for attached networks not having a Gs-interface. In compliance with the standard, the SGSN rejects an Attach in a MOCN configuration with cause 'CS-PS coordination required', after learning the IMSI, to facilitate the RNC choosing the same operator for both CS and PS domains.

Example

Use the following syntax to disable the CS-PS coordination check:

```
no network-sharing cs-ps-coordination
```

nri length

This command defines the Network Resource Identifier (NRI) of the SGSN that is stored in the P-TMSI (bits 23 to 18).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
nri length  nri_length { nri-value nri_value | null-nri-value null_nri_value non-
broadcast mcc mcc mnc mnc lac lac_id rac  rac_id [ nri-value value }

no nri
```

no

Removes the configured NRI value and location in P-TMSI for retrieval by this operator policy.

nri length *nri_length*

Specifies the number of bits to be used in the P-TMSI, bits 23 to 18. to define the network resource identifier (NRI). The NRI length configuration also sets the maximum size of the pool. If not configured, the NRI length will be of zero length.
nri_length : Must be an integer from 1 to 6 to identify the number of bits.

null-nri-value *null_nri_value*

This keyword is only available in releases 8.1 and higher.
Configures the null NRI value which must be unique across the pool areas. This keyword is used for the offloading procedure for SGSN pooling (enabled with the **sgsn offloading** command, see the Exec Mode chapter).
null_nri_value : 0 (zero) indicates the keyword is not to be used and 1 to 63 are used to identify the SGSN to be used for the offloading procedure for SGSN pooling. There is no default value for this parameter.

non-broadcast mcc *mcc* **mnc** *mnc* **lac** *lac_id* **rac** *rac_id*

This keyword set is only available in releases 8.1 and higher.
Defines the non-broadcast LAC/RAC to be used in combination with the null-NRI for the offloading procedure. Including the MCC and MNC to specify the PLMN because the Iu-Flex feature supports multiple IuPS Services.
mcc identifies the mobile country code, the first part of the PLMN ID. Must be an integer between 100 and 999.
mnc identifies the mobile network code portion of the PLMN ID. Must be a 2- or 3-digit integer between 01 and 999.
lac_id defines a location area code associated with an RNC. Must be an integer between 1 and 65535.
rac_id defines the remote area code to be associated with an RNC. Must be an integer between 1 and 255.

nri-value *nri_value*

Specifies the MS-assigned value of the NRI to retrieve from the P-TMSI. This value must not exceed the maximum possible value specified by the NRI length. The NRI value must be unique across the pool or across all overlapping pools.

nri_value must be an integer from 1 to 63 to identify a specific SGSN in a pool. Use of 0 (zero) value is not recommended.
Multiple NRI values can be identified by providing multiple nri-values separated by a blank space for example: **nri length** *6* **nri-value** *29 43 61*

Usage

Use this command to identify the SGSN identified with the NRI in the MS generated P-TMSI.
This command adds or removes the Iu Flex configuration for this SGSN service. When using Iu Flex, all keywords must be defined. The command can be repeated to specify different values for any of the keyword parameters. If more than one NRI is configured, the SGSN service will round-robin between the available NRIs when new subscribers (re)connect.
Use this command to retrieve the NRI (identity of an SGSN) stored in in bits 23 to 18 of the packet-temporary mobile subscriber identity (P-TMSI). If more than one NRI value is configured, the SGSN service will round-robin between the available NRIs when new subscribers (re)connect.
When using MOCN mode for network sharing without SGSN pooling, the NRI length and the NRI value should both be used.

Example

The following command specifies the the NRI length as 5 bits, identifies SGSN 23 with LAC 222 and RAC 12 for offloading procedure with NRIs 6 and 41:

```
nri length 5 null-nri-value 34 non-broadcast lac 222 rac 12 nri-value 6
41
```

override-lac-li

Refer to the *ASR 5000 Lawful Intercept Guide* for a description of thsi command.

override-rac-li

Refer to the *ASR 5000 Lawful Intercept Configuration Guide* for a description of this command.

rac

Refer to the *ASR 5000 Lawful Intercept Configuration Guide* for a description of this command.

ran-protocol

This command specifies the IuPS service for the SGSN service to use for communication with the RAN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ran-protocol iups-service *iups_srvc* **[context** *ctx_name*]

no ran-protocol iups-service

no

Removes the IuPS service information from the SGSN service configuration.

iups-service *iups_srvc*

Specifies the name of an IuPS service already configured on the system.
iups_srvc : Enter an alphanumeric string of 1 to 63 characters.

ctx_name

ctx_name : Enter the name of the IuPS context, an alphanumeric string of 1 to 63 characters.

Usage

Use this command to configure the IuPS service context that the current SGSN service will use to communicate with the RAN. Up to 8 definitions can be defined for a single SGSN service to allow for multiple PLMNs support.

Example

The following command configures the SGSN service to use an IuPS service named **iups1** that has been configured. in the same context as the SGSN service:

```
ran-protocol iups-service iups1
```

reporting-action event-record

This command enables the SGSN to log GMM/SM events in EDR files for 3G services.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
reporting-action event-record

[ default | no ] reporting-action event-record
```

default

Disables the logging function.

no

Removes the logging function from the configuration file.

Usage

This command is one of the steps needed to enable the SGSN to create a log for events such as Attach, RAU, and Activations. The log is an EDR (event data record) in CSV format. For details about how this feature works, refer to the *GMM-SM Event Logging* chapter in the *SGSN Administration Guide*.

Related Commands:

- To enable GMM/SM event logging for 2G services, the **reporting-action event-record** command must be configured in the GPRS service configuration.
- To enable a log to be generated in an EDR file, the **edr-module active-charging-service** command must be enabled in the Context configuration mode.
- To configure parameters for the logging file characteristics and for file transfer, use the commands in the EDR Module Configuration Mode.

Example

Enable GMM/SM event logging for 3G services:

```
reporting-action event-record
```

sgsn-number

This command defines the E.164 number that identifies this particular SGSN service context.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sgsn-number *E.164_number*

no sgsn-number

no

Removes the SGSN number configuration from the SGSN service configuration.

E.164_number

Enter a maximum of 15 digits to define the 'phone' number associated with this SGSN service in the specified context.

Usage

The SGSN supports multiple SGSN numbers – different numbers in the 2G GPRS service configuration and the the 3G SGSN service configuration. If an HLR-initiated dialog is received, the SGSN will perform a lookup based on the IMSI and find the correct SGSN number with which the MS is associated. Subsequent messaging will use this address.

Example

To delete the sgsn-number associated with this SGSN service context, enter:

```
no sgsn-number
```

sgtp-service

This command creates an instance of an SGTP service.

Product

SGSN

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

sgtp-service *sgtp_srvc_name*

no sgtp-service

sgtp_srvc_name

Enter the name of an SGTP service that will be used by this SGSN service
sgtp_srvc_name : Enter a string of 1 to 63 alphanumeric characters.

Usage

Use this command to access the SGTP Service configuration mode to configure SGTP parameters.

Example

sgtp-service *sgtp1*

sm

This command configures session management parameters for this SGSN service. This command can be repeated multiple times to configure each parameter individually.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

sm { T3385-timeout *time* **| T3386-timeout** *time* **| T3395-timeout***time* **| max-actv-retransmission** *number* **| max-deactv-retransmission** *number* **| max-modf-retransmission** *number* **}**

default sm *timer*

default

Resets the selected timer to the system default value.

T3385-timeout

Retransmission timer for network-initiated Activate Request. Default is 8 sec

T3386-timeout

Retransmission timer for network-initiated Modify Request. Default is 8 sec

T3395-timeout

Retransmission timer for network-initiated Deactivate Request. Default is 8 sec

max-actv-retransmission

Configures maximum retries for activate PDP ctxt request. Default is 4

max-deactv-retransmission

Configures maximum retries for deactivate PDP ctxt request. Default is 4

max-modf-retransmission

Configures maximum retries for modify PDP ctxt request. Default is 4

Usage

Repeat the command to configure multiple session management parameters for the SGSN service.

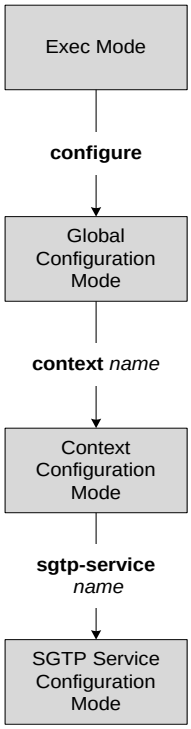
Example

```
sm T3385-timeout 5
```

Chapter 255
SGTP Service Configuration Mode Commands

The SGSN GPRS Tunneling Protocol (SGTP) Service configuration mode provides the configuration of GTP-C and GTP-U related parameters.

[<*ctx_name*>]*hostname*(config-sgtp-service)#



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

direct-tunnel-disabled-ggsn

This command makes it possible for the operator to disable direct tunneling on the basis of a GGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

direct-tunnel-disabled-ggsn *IPv4/IPv6_address*

no direct-tunnel-disabled-ggsn [*IPv4/IPv6_address* **]**

no

Deletes the direct-tunnel-disabled-ggsn configuration which results in re-enabling direct tunneling to the GGSN.

- Including an IPv4 or IPv6 address for a specific GGSN, re-enables direct tunneling for that specific GGSN.
- Excluding any IPv4 or IPv6 address from this command removes all direct-tunnel-disabled-ggsn definitions from the SGTP service configuration.

Usage

By default, GGSNs and RNCs are assumed to be capable of direct tunneling.
This command disables direct tunneling for a specified GGSN. The command can be repeated to disable direct tunneling for multiple GGSNs, thereby creating a 'disabled GGSN' list. Checking for a direct-tunnel-disabled GGSN is actually the last step in the PDP Activation procedure.
Restricting direct tunneling by a GGSN for an entire APN would be configured with the appropriate command in the APN profile configuration mode.
Restricting direct tunneling at the RNC level would be configured with the appropriate command in the IuPS service configuration mode.
This command can only be used if:

- The Direct Tunnel license has been purchased and applied.
- The Direct Tunnel feature is appropriately enabled via configurations of the IMEI profile and/or the Call-Control and APN profiles.
- The RNC does not restrict direct tunnel.
- The subscriber is not requesting CAMEL services.

Example

Use the following command to disable direct tunnel for the GGSN with the IP address of *141.21.4.20*:

```
direct-tunnel-disabled-ggsn 141.21.4.20
```

disable-remote-restart-counter-verification

This command disables the SGSN's default behavior for verification of the remote peer's (GGSN) restart counter change values.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
disable-remote-restart-counter-verification

[ default | no ] disable-remote-restart-counter-verification
```

default

Enables the default behavior for verification of the GGSN's restart counter change values.

no

Disables the command configuration and enables the default behavior of verification.

Usage

This command disables the default behavior used to minimize PDP deactivations resulting from path failure detection due to erroneous restart counter change messages.

With the execution of this command, the SGSN stops verifying restart counters received in Create PDP Context Response or Update PDP Context Response or Update PDP Context Request (CPCR, CPCR, and UPCQ) messages. When the SGSN detects GTP-C path failure between the SGSN and the GGSN, the SGSN assumes PDP sessions at the GGSN are lost and the SGSN deactivates those PDP sessions towards the UE with an indication that the UE should activate the PDP session again. Potentially, this scenario could cause unnecessary traffic increases within the operator's network.

The SGSN default behavior provides the ability to manage GTP-C path failures detected as a result of spurious restart counter change value messages received from the GGSN. With the default behavior, path failure detection is based on receipt of restart counter change values in CPCR, CPCR, and UPCQ messages. The session manager informs the SGTPC manager about a changed restart counter value. The SGTPC manager verifies the PDP context status by performing an echo request and echo response with the GGSN. Only then is the path failure confirmed if the echo response contains a new restart counter value. Then the SGTPC manager informs all session managers about the path failure and the session managers begin deactivation of the PDP contexts.

Related commands:

- **max-remote-restart-counter-change**, also part of the SGTP service configuration mode, allows the operator to set a maximum variance between stored and received values for restart counter changes coming from the GGSN.
- **pdp-deactivation-rate**, in the SGSN Global configuration mode, allows the operator to modify the rate the SGSN deactivates PDP connections when GPT-C path failure is detected.
- **ignore-remote-restart-counter**, also part of the SGTP service configuration mode.

Example

Disable the default behavior and stop verification with echo request/response process:

```
disable-remote-restart-counter-verification
```

Use either of the following commands to enable the default verification behavior:

```
no disable-remote-restart-counter-verification
```

```
default disable-remote-restart-counter-verification
```

end

Exits the configuration mode and returns to the Exec mode.

Product

SGSN

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Changes the mode to the Exec mode.

exit

Exits the SGTP Service configuration mode and returns to the Context configuration mode.

Product

SGSN

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Return to the previous mode.

ggsn-fail-retry-timer

This command sets the amount of time that a GGSN will be unavailable.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

ggsn-fail-retry-timer *value*

no ggsn-fail-retry-timer

no

Removes the timer setting and disables the Local DNS feature.

value

Defines the amount of time, in seconds, that the GGSN is to be considered unavailable.
Enter an integer from 60 to 600. Default is 300.

Usage

Setting this timer to a valid value enables the Local DNS feature - described in the *SGSN Administration Guide*. Setting this timer marks a GGSN in the primary GGSN pool as unavailable for PDP context creation and causes the SGSN to forward a PDP Context Activation Request to a remote pool GGSN, identified via a local (on the SGSN) DNS check. Marking a GGSN unavailable can be done if there is a reason to believe the GGSN is unavailable; for example, lack of response to GTP messages. Marking a GGSN as unavailable is usually done for a limited period to allow the GGSN time to recover.

Example

Enable the Local DNS feature and mark the GGSNs in the primary pool as unavailable for 4 minutes (*240 seconds*):

```
ggsn-fail-retry-timer 240
```

gn-delay-monitoring

This command configures monitoring of Gn/Gp interface to check for the delay of packets between the SGSN and the GGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

gn-delay-monitoring [num-delay *number_delayed* **| num-no-delay-for-clear** *number_normal* **| tolerance-seconds** *number_seconds* **]**

default gn-delay-monitoring [num-delay | num-no-delay-for-clear | tolerance-seconds]

no gn-delay-monitoring

default

Resets the specified parameter to the default value.

no

Disables Gn/Gp monitoring for delayed GTP-C packets.

num-delay *number_delayed*

Defines the number of response messages, coming from the GGSN, that can be delayed (delay time defined by tolerance-seconds parameter) before the delay is flagged to generate an SNMP trap.
number_delayed: Enter an integer from 1 to 500, default is 30.

num-no-delay-for-clear *number_normal*

Defines the number of consecutive response messages, coming from the GGSN, that must be received without delay (in normal response time) to clear the flag towards the GGSN.
number_normal: Enter an integer from 1 to 500, default is 15.

tolerance-seconds *number_seconds*

Defines the 'normal' number of seconds the SGSN should wait for a response from the GGSN. After this time, the response would be considered 'delayed'.
number_seconds: Enter an integer from 1 to 20, default is 4 seconds.

Important: The value for this parameter should be less than the value set for the **retransmission-timeout** parameter of the **gtpc** command, also in this configuration mode.

Usage

With this command, the SGSN can monitor the control plane packet delay for GTP-C signaling messages on the SGSN's Gn/Gp interface towards the GGSN. If the delay crosses this configurable threshold, an alarm will be generated to prompt the operator.
A delay trap is generated when the GGSN response to an ECHO message request is delayed more than a configured amount of time and for a configured number of consecutive responses. When this occurs, the GGSN will be flagged as experiencing delay.
A clear delay trap is generated when successive ECHO Response (number of successive responses to detect a delay clearance is configurable), are received from a GGSN previously flagged as experiencing delay.
This functionality can assist with network maintenance, troubleshooting, and early fault discovery.

Example

Enable Gn/Gp monitoring for GTP-C packets that arrive from the GGSN with a delay greater than *5* seconds:

```
gn-delay-monitoring tolerance-seconds 5
```

gtpc

Configure the GPRS Tunneling Protocol Control (GTP-C) settings for the SGTP service.

Product

SGSN

MME

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

gtpc { bind address *ip_address* **| dns-sgsn context** *cntxt_name* **| echo-interval** *seconds* **| guard-interval** *seconds* **| ignore response-port-validation | ip qos-dscp** *<dscp_marking>* | max-retransmissions *num* **| retransmission-timeout** *seconds* **| send { common flags | rab-context | target-identification-preamble } }**

no gtpc { bind address ip_address | dns-sgsn context *cntxt_name* **| echo-interval** *seconds* **| send { common- flags | rab-context | target-identification-preamble } }**

default gtpc { echo-interval | guard-interval | ignore response-port-validation | ip qos-dscp | max-retransmissions | retransmission-timeout | send { common-flags | rab-context | target-identification-preamble } }

---

no

Disables the configured GTPC setting.

---

default

Resets the specified parameter to its default value.

---

bind address *ip_address*

Binds SGTP service to the IP address of the interface.
The bind address for the **gtpc** and **gtpu** commands should be the same.
ip_address: Enter a standard dotted-quad IPv4 address.

---

dns-sgsn context *cntxt_name*

Enter a string of 1 to 79 alphanumeric characters to identify the context.

---

echo-interval *seconds*

Configures the duration between echoes.
seconds: Enter an integer from 0 through 3600.
Default: 60

guard-interval *seconds*

Configures the interval (in seconds) for which the SGTP maintains responses sent to SGSN. This optimizes the handling of retransmitted messages. This value should be configured to be greater than the SGSN's configuration for max-retries multiple by retry-interval.
seconds: Enter an integer from 10 to 3600.
Default: 100

ignore response-port-validation

This keyword instructs the SGSN to ignore the response port validation.
For the SGSN to process incoming GTP responses to an *incorrect* port,

- this keyword must be entered, and
- the same **bind address** must be configured for GTPC and GTPU in the SGTP service.

Default: disabled. To reset the default for this parameter, you must enter the following command: **no gtpc ignore response-port-validation**.

ip qos-dscp *<dscp_marking>*

Configures the diffserv code point marking to be used when sending GTP-C messages originating from the session manager and SGTPC manager.
<dscp_marking>: Enter one of the following values:

- **af11**: Marks traffic as Assured Forwarding 11 PHB (high throughput data)
- **af12**: Marks traffic as Assured Forwarding 12 PHB (high throughput data)
- **af13**: Marks traffic as Assured Forwarding 13 PHB (high throughput data)
- **af21**: Marks traffic as Assured Forwarding 21 PHB (low latency data)
- **af22**: Marks traffic as Assured Forwarding 22 PHB (low latency data)
- **af23**: Marks traffic as Assured Forwarding 23 PHB (low latency data)
- **af31**: Marks traffic as Assured Forwarding 31 PHB (multimedia streaming)
- **af32**: Marks traffic as Assured Forwarding 32 PHB (multimedia streaming)
- **af33**: Marks traffic as Assured Forwarding 33 PHB (multimedia streaming)
- **af41**: Marks traffic as Assured Forwarding 41 PHB (multimedia conferencing).
- **af42**: Marks traffic as Assured Forwarding 42 PHB (multimedia conferencing)
- **af43**: Marks traffic as Assured Forwarding 43 PHB (multimedia conferencing)
- **be** : Designates use of Best Effort forwarding PHB. This is the default value.
- **ef** : Designates use of Expedited Forwarding PHB

Default: **be** (best effort)

max-retransmissions *num*

Configures the maximum number of retries for packets.
num: Enter an integer from 0 to 15.
Default: 4

retransmission-timeout *seconds*

Configures the control packet retransmission timeout in GTP, in seconds.
seconds: Enter an integer value from 1 through 20.

Default: 5

send { common-flags | rab-context | target-identification-preamble }

common-flags : This option configures the SGTP service to include or exclude the common flags IE during an Inter-SGSN RAU. When selected, the default is to send the common flags IE.
rab-context : This option configures the SGTP service to include/exclude the radio access bearer (RAB) context IE in SGSN 'context response' message during Inter-SGSN Routing Area Update procedure. Default is to send the RAB context IE.
Default: RAB context IE.
target-identification-preamble : This option configures the SGTP service to include the preamble byte in the target-id of Relocation Requests that it sends. By default, the preamble is not included.

Important: Sending of common flags must be enabled to configure dual PDP type (IPv4v6) addressing with the **dual-address-pdp** command in the SGSN global configuration mode.

Usage

Use this command to configure GTP-C settings for the current SGTP service.

Example

Following command excludes the radio access bearer (RAB) context IE in the SGSN Context Response message during the inter-SGSN RAU procedure:

```
no gtpc send rab-context
```

Configure the SGSN to send *common flags* with all GTP-C messages:

```
gtpc send common-flags
```

gtpu

This command configures the GPRS Tunneling Protocol user data plane parameters (GTP-U) for this SGTP service.

Product

SGSN

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

```
gtpu { bind address ip_address | echo-interval | max-retransmissions | retransmission-
timeout } +

no gtpu { bind | echo-interval }

default gtpu { echo-interval | max-retransmissions | retransmission-timeout }
```

no

Removes the configuration for the specified parameter from the current SGTP service configuration.

default

Resets the specified GTP-U parameter to its factory default.

bind address *ip_address*

Defines the GTP-U Gn interface IP address that binds to this SGTP service.
The **gtpu** and the **gtpc** commands should be configured with the same bind address.
ip_address: Enter a standard dotted-quad IPv4 address.

echo-interval *seconds*

Configures the echo interval.
seconds: Enter an integer from 60 through 3600.
Default: 60

max-retransmissions *num*

Configures the maximum number of retries for retransmitting packets.
num: Enter an integer from 0 through 15.
Default: 4

retransmission-timeout *seconds*

Configures the retransmission timeout of packets, in seconds.
seconds: Enter an integer from 1 through 20.
Default: 5

Usage

Use this command to configure the GTP-U settings for the SGTP service.

Example

Set the GTPU echo-interval for *5* seconds:

```
gtpu echo-interval 5
```

ignore-remote-restart-counter-change

With the inclusion of the **disable-remote-restart-counter-verification** command, this command has been deprecated.

max-remote-restart-counter-change

Use this command to set a restart counter change window to avoid service deactivations and activations that could cause large bursts of network traffic if the restart counter change messages from the GGSN are erroneous

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

max-remote-restart-counter-change *variance*

default max-remote-restart-counter-change

default

If this keyword is used or if a variance window is not configured, then the default value will be 255 and the default behavior of the SGSN will be to detect a restart on any change.

variance

Set a number (an 8-bit value) that will define the variance range for restart counter change values compared between the SGSN's stored value and the value received in messages from the GGSN. Valid entry is an integer from 1 to 255; default is 255.
Value of 32 is recommended as it provides a sufficient window to allow the SGSN to handle delayed messages with old restart counters.

Usage

When the SGSN detects GTP-C path failure between the SGSN and the GGSN, the SGSN assumes PDP sessions at the GGSN are lost and the SGSN deactivates corresponding PDP sessions towards the UE with an indication that the UE should activate the PDP session again. Detection is based on receipt of restart counter change values in Create PDP Context Response or Update PDP Context Response or Update PDP Context Request (CPCR/UPCR/UPCQ) messages. Potentially, this scenario can cause major traffic increases within the operator's network. It is possible that the messages received from the GGSN are spurious.
The SGSN default behavior provides the ability to verify possible GTP-C path failures detected as a result of spurious restart counter change messages received from the GGSN. With the default behavior, the session manager informs the SGTPC manager about a changed restart counter value. The SGTPC manager responds by verifying the PDP context status by performing an Echo Request / Echo Response with the GGSN. If the Echo Response includes a new restart counter change value, then the session manager considers the path failure confirmed and begins the PDP context deactivation sequence.
Use this command to avoid unnecessary path failures and deactivations by setting a restart counter change value ‘window’ or range of values. With this window, the SGSN only accepts linearly increasing values for restart counter change values that are within the specified range of accepted changes before the SGTPC manager verifies. For example, if the allowed window for restart counter change value is set to 32 and the last learnt restart counter change value from the GGSN is 15, then the SGSN should detect a restart only if the new restart counter value is between 16 and 47 (range of 32) and then the SGSN would verify with the Echo Request/Response. If the received restart counter change value was 200 and the current learnt value was 15 with a window of 32, then the 200 would be ignored as a spurious value.

Also, use this command to set a restart counter change values window to avoid possible 'race conditions' (as defined in 3GPP TS 23.007 v8.7.0) where a new message arrives prior to an older message. This 'race condition' occurs when the SGSN's stored restart counter value for the GGSN is larger than the restart counter value received in the messages received from the GGSN.

Related commands:

- **`disable-remote-restart-counter-verification`** - also part of the SGTP service configuration mode, this command allows the operator to disable the default behavior.
- **`pdp-deactivation-rate`**, in the SGSN Global configuration mode, this allows the operator to modify the rate the SGSN deactivates PDP connections when GPT-C path failure is detected.
- **`ignore-remote-restart-counter`**, also part of the SGTP service configuration mode.

Example

Use the following command to configure an allowed restart counter change value window of *32*:

```
max-remote-restart-counter-change 32
```

mbms

Enables / disables the Multimedia Broadcast Multicast Service

Important: The **mbms** command and parameter-configuring keywords are under development for future release and should not be used or included in your configuration at this time.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

mbms

Usage

path-failure

This command specifies the method for determining if path failure has occurred.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

path-failure detection-policy gtp *type*

[default | no] path-failure detection-policy

default

Resets the specified path failure parameter to default.

no

Deletes the path-failure definition from the configuration.

detection-policy gtp *type*

Specifies the policy to be used, value options include:

- **echo** - When set to 'echo', path failure is detected when the retries of echo messages time out.
- **non-echo** - When set to 'non-echo', path failure is detected when the retries of non-echo messages time out.

Default: echo (for both GTPC and GTPU)

Usage

Use this command to define the policy to detect gtp path failure.

Example

Set *echo* as the polity detection type:

```
path-failure detection-policy gtp echo
```

pool

This command enables the default SGSN functionality for (flex) pooling and enables inclusion of the configured pool hop-counter count in new SGSN context/identify request messages.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
pool { default-sgsn | hop-counter count }

no pool { default-sgsn | hop-counter }

default pool hop-counter
```

no

Disables the default SGSN pooling functionality or removes the SGSN pool hop-counter IE from the GTP Identity/context requests.

default

Removes the SGSN pool hop-counter IE from the GTP Identity/context requests.

default-sgsn

Enables default SGSN pooling functionality.

hop-counter *count*

Enables and configures the SGSN pool hop-counter to set the number of hops and to include the configured count in the **new** SGSN Context Requests or the **new** SGSN Identify Requests.
If **default-sgsn** is enabled, then any messages relayed will have the default value of 4 for the counter if the message does not include this hop-counter ID.
count: Enter an integer from 1 to 255.
Default: 4

Usage

Use this command to enable the default flex functionality without exposing the pool (flex) structure. This functionality provides a means for SGSNs outside of the pool to reach a pooled SGSN on the basis of its NRI. Once the pooling has been enabled. Repeat the command using the **hop-counter** keyword to enable inclusion of the hop-counter IE in SGSN context/identify request messages and to configure the count for the pooling hop-counter. If the SGSN is behaving as the 'default SGSN', this SGSN will forward (relay) requests with the hop-count included to the target SGSN.

Example

Enable the default pooling functionality which allows an outside SGSN to reach a pooled SGSN:

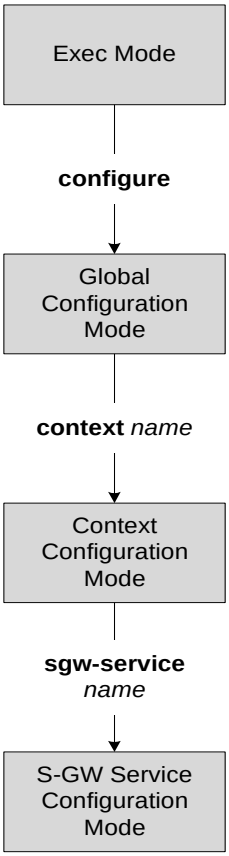
```
pool default-sgsn
```

Set the hop-count to be included in messages to *25*:

pool hop-count

Chapter 256
S-GW Service Configuration Mode Commands

The S-GW (Serving Gateway) Service Configuration Mode is used to create and manage the relationship between an eGTP service used for either ingress or egress control plane and user data plane network traffic.



accounting context

Configures the GTPP accounting context and group selection for S-GW service.

Product

S-GW

Privilege

Administrator

Syntax

accounting context *name* **[gtpp group** *name* **]**

no accounting context

---

no

Removes the configured accounting context from this service.

---

context *name*

Specifies the context where GTPP accounting is performed. *name* must be an existing context configured on the system expressed as an alphanumeric string of 1 through 79 characters.
If an accounting context name is not configured in the S-GW service, the context where the S-GW service resides is considered the accounting context and the default GTPP group is used.

---

gtpp group *name*

Specifies a GTPP group used to perform GTPP accounting. *name* must be an existing GTPP group configured on the system expressed as an alphanumeric string of 1 through 79 characters.
If a GTPP group is not configured, the system will use the default GTPP group in the specified accounting context. If the accounting context is not specified, the system will use default GTPP group in the context where the S-GW service resides.

Usage

Use this command to specify the accounting context and/or GTPP accounting group the S-GW service will use to perform GTPP accounting.

Example

The following command specifies a GTPP accounting context named *acct-2* and a GTPP accounting group named *gtpp-grp-3* as the context and group the S-GW service will use:

```
accounting context acct-2 gtpp group gtpp-grp-3
```

accounting mode

Configures the mode to be used for accounting – GTPP (default), RADIUS/Diameter or None for S-GW service.

Product

S-GW

Privilege

Administrator

Syntax

```
[ default ] accounting mode { gtpp | none | radius-diameter }
```

default

Sets the accounting mode to GTPP.

gtpp

Specifies that GTPP accounting is performed. This is the default mode.

none

Specifies that no accounting will be performed for the S-GW service.

radius-diameter

Specifies that RADIUS/Diameter will be performed for the S-GW service.

Usage

Use this command to specify the accounting mode for the S-GW service. However, an accounting mode configured for the call-control profile will override this setting. For additional information on accounting mode and its relationship to operator policy, refer to the *Serving Gateway Administration Guide*.

Example

The following command specifies that RADIUS/Diameter accounting will be used for the S-GW service:

```
accounting mode radius-diameter
```

associate

Associates the S-GW service with QoS and policy control and charging configurations.

Product

S-GW

Privilege

Administrator

Syntax

associate { accounting-policy *name* **| egress-proto { gtp | gtp-pmip | pmip } [egress-context** *name* **[egtp-service** *name* **] [mag-service** *name* **]] | ims-auth-service** *name* **| ingress egtp-service** *name* **| qci-qos-mapping** *name* **| subscriber-map** *name*

no associate { accounting-policy | egress-proto [egress-context [egtp-service] [mag-service]] | ims-auth-service | ingress egtp-service | qci-qos-mapping | subscriber-map }

no

Removes the specified association form the S-GW service.

accounting-policy *name*

Associates the S-GW service with an accounting policy configured in the same context. *name* must be an existing accounting policy expressed as an alphanumeric string of 1 through 63 characters.
Accounting policies are configured through the **policy accounting** command in the Context Configuration Mode.

egress-proto { gtp | gtp-pmip | pmip } [egress-context *name* **[egtp-service** *name* **] [mag-service** *name* **]]**

Associates and configures the egress protocol for this S-GW service.
gtp: Specifies that GTP is to be used for the S-GW service egress.
gtp-pmip: Specifies that either GTP or PMIP is to be used for the S-GW service egress.
pmip: Specifies that PMIP is to be used for the S-GW service egress.
egress-context *name*: Specifies that the context in this keyword is to be used for the S-GW service egress. *name* must be an existing context on this system expressed as an alphanumeric string of 1 through 63 characters.
egtp-service *name*: Specifies that the service in this keyword is to be used for the S-GW service egress. *name* must be an existing eGTP service on this system expressed as an alphanumeric string of 1 through 63 characters.
mag-service *name*: Specifies that the service in this keyword is to be used for the S-GW service egress. *name* must be an existing MAG service on this system expressed as an alphanumeric string of 1 through 63 characters.

ims-auth-service *name*

Associates the S-GW service with an IMS authorization service configured in the same context. *name* must be an existing IMS auth service and be from 1 to 63 alphanumeric characters.
IMS authorization services are configured through the **ims-auth-service** command in the Context Configuration Mode.

ingress egtp-service *name*

Associates and configures the eGTP service ingress for this S-GW service. *name* must be an existing eGTP service on this system expressed as an alphanumeric string of 1 through 63 characters.

qci-qos-mapping *name*

Associates the S-GW service with QCI to QoS mapping parameters. *name* must be an existing QCI-QoS mapping configuration expressed as an alphanumeric string of 1 through 63 characters.
QCI-QoS mapping is configured through the **qci-qos-mapping** command in the Global Configuration Mode.

subscriber-map *name*

Associates the S-GW service with subscriber map parameters. *name* must be an existing subscriber map configuration expressed as an alphanumeric string of 1 through 63 characters.
Subscriber maps are configured through the **subscriber-map** command in the LTE Policy Configuration Mode.

Usage

Use this command to select a pre-configured QoS mapping and/or policy control and charging configuration to be used by the S-GW service.

Example

The following command associates the S-GW service with an IMS authorization service named *ims-23*:

```
associate ims-auth-service ims-23
```

ddn

Configures a timer that determines how long the S-GW will discard downlink data packets so the MME has enough time to receive the Modify Bearer Request and prevent further errors being sent to the S-GW in the DDN Ack message.

Product

S-GW

Privilege

Administrator

Syntax

ddn failure-action pkt-drop-time *seconds*

default ddn failure-action pkt-drop-time

default

Resets the command to its default setting of 300 seconds.

failure-action pkt-drop-time *seconds*

Default: 300
Specifies the time, in seconds, to multiply with the delay value IE sent from the MME. *seconds* must be an integer value from 1 to 300.

Usage

Use this command to set a timer value to delay the sending of excessive Downlink Data Notification messages to the MME (and receiving excessive DDN Ack message with errors from the MME) in cases when downlink data is arriving before the Modify Bearer Request is received. During the delay, downlink data packets are discarded until the timer has expired. This timer is triggered upon receiving the first error in a DDN Ack message from the MME.

Example

The following command sets the base factor used to calculate the packet drop timer to *200* seconds:

```
ddn failure-action pkt-drop-time 200
```

egtp-service

Configures an eGTP service to use as either an ingress (S1-U) or egress (S5/S8) service for the S-GW.

Product

S-GW

Privilege

Administrator

Syntax

```
egtp-service { egress { context name | service name } | ingress service name }

no egtp-service { egress { context | service } | ingress service }
```

no

Removes the selected EGTP service from this service.

egress { context *name* **| service** *name* **}**

Specifies the egtp-service to be used as the egress eGTP service on a GTP-based S5/S8 interface.
context *name*: Specifies the name of the context where the eGTP service resides. *name* must be an existing context name where an eGTP service resides expressed as an alphanumeric string of 1 through 63 characters.

Caution: **context** *name* is not supported in this release.

service *name*: Specifies the name of the egress eGTP service. *name* must be an existing eGTP service name expressed as an alphanumeric string of 1 through 63 characters.

ingress service *name*

Specifies the egtp-service to be used as the ingress eGTP service on the S11 interface. *name* must be an existing eGTP service name expressed as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the eGTP service to use with this S-GW service. The eGTP service must be existing and be configured with the appropriate parameters supporting the intended service type.

Example

The following command configures the S-GW service to use an eGTP service named *s1u-egtp* as its ingress service:

```
egtp-service ingress service slu-egtp
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

gtpu-error-ind

Configures the actions to be taken upon receiving a GTP-U error indication from an RNC, eNodeB, SGSN, or P-GW.

Product

S-GW

Privilege

Administrator

Syntax

```
gtpu-error-ind { { s12 | s1u } { local-purge | page-ue [ custom1-behavior ] } | { s4u |
s5u } { local-purge | signal-peer } }

default gtpu-error-ind { s12 | s1u | s4u | s5u }
```

default

Resets the command to the default action for the specified interface. For S12 and S1-U, **page-ue** is the default action. For S4-U and S5-U, **local-purge** is the default action.

{ s12 | s1u } { local-purge | page-ue [custom1-behavior] }

Specifies the action to take when a GTP-U error indication is received from a Radio Network Controller (RNC) over an S12 interface or from an eNodeB over the S1-U interface.
local-purge: The S-GW clears the affected bearer (or PDN if error-indication is received on default bearer) locally without informing peer.
page-ue [custom1-behavior]: The S-GW moves the complete UE state to S1-Idle and starts paging for this UE. If the custom1-behavior option is specified, the S-GW will guard the paging attempt with a timer of 60 seconds. Within this time the bearer must have the eNodeB TEID refreshed by an MME. Otherwise, the S-GW will clear the affected bearer with signaling. This is the default action for GTP-U error indication messages received on the S12 and S1-U interfaces.

{ s4u | s5u } { local-purge | signal-peer }

Specifies the action to take when a GTP-U error indication is received from an SGSN over an S4-U interface or from a P-GW over the S5-U interface.
local-purge: The S-GW clears the affected bearer (or PDN if error-indication is received on a default bearer) locally without informing the peer. This is the default action for GTP-U error indication messages received on the S4-U and S5-U interfaces.
signal-peer: The S-GW initiates control signalling towards the peer MME and P-GW. When signalling:

- For a bearer deletion, the S-GW sends a Delete-Bearer-Command message to the P-GW and a Delete-Bearer-Request (with EBI) message to the MME.
- For PDN deletion, the S-GW sends a Delete-Session-Request message to the P-GW and a Delete-Bearer-Request (with LBI) message to the MME.
- The S-GW will not wait for Delete replies from the peer. The request will be sent only once and local resources will be reset.

Usage

Use this command to specify the action to taken upon receiving a GTP-U error indication from an RNC over an S12 interface, an eNodeB across an S1-U interface, an SGSN over an S4-U interface, or from a P-GW across an S5-U interface.

Example

The following command sets the action to take upon receipt of a GTP-U error indication from the eNodeB to clear affected bearer:

```
gtpu-error-ind s1u local-purge
```

mag-service

Identifies the Mobile Access Gateway (MAG) egress service through which calls are to be routed for this S-GW service.

Product

S-GW

Privilege

Administrator

Syntax

mag-service egress service *name*

no mag-service egress service

no

Removes the configured MAG egress service from this service.

egress service *name*

Specifies the MAG service name to be used as the egress MAG service on a Proxy Mobile IPv6 (PMIP) based S5/S8 interface. *name* must be an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify the name of the MAG service where calls are to be routed.

Example

The following command specifies that an existing MAG service named *mag3* is to be used to route call through for this S-GW service:

```
mag-service egress service mag3
```

path-failure

Configures the action to take upon the occurrence of a path failure between the S-GW and the MME, P-GW, RNC, SGSN, or eNodeB.

Product

S-GW

Privilege

Administrator

Syntax

```
path-failure { s11 | s12 | s1u | s4 | s4u | s5 | s5u } ( local-purge | signal-peer }

default path-failure { s11 | s12 | s1u | s4 | s4u | s5 | s5u }
```

default

Returns the command to the default setting of "local purge" for the selected interface.

{ s11 | s12 | s1u | s4 | s4u | s5 | s5u }

Specifies the interface to which the action will be applied.
s11: Applies the path failure action to the S11 interface between the S-GW and the MME.
s12: Applies the path failure action to the S12 interface between the S-GW and the RNC.
s1u: Applies the path failure action to the S1-U interface between the S-GW and the eNodeB.
s4: Applies the path failure action to the S4 control plane interface between the S-GW and the SGSN.
s4u: Applies the path failure action to the S4-U user plane interface between the S-GW and the SGSN.
s5: Applies the path failure action to the S5 interface between the S-GW and the P-GW.
s5u: Applies the path failure action to the S5-U user plane interface between the S-GW and the P-GW.

{ local-purge | signal-peer }

Specifies the action to apply to the selected interface.
local-purge: The S-GW clears the affected bearer (or PDN if path failure is received on a default bearer) locally without informing the peer. This is the default action for all interface.
signal-peer: The S-GW initiates control signalling towards the peer MME and P-GW. When signalling:

- For a bearer deletion, the S-GW sends a Delete-Bearer-Command message to the P-GW and a Delete-Bearer-Request (with EBI) message to the MME.
- For PDN deletion, the S-GW sends a Delete-Session-Request message to the P-GW and a Delete-Bearer-Request (with LBI) message to the MME.
- The S-GW will not wait for Delete replies from the peer. The request will be sent only once and local resources will be reset.

Usage

Use this command to specify the type of action to take when a path failure occurs on one of the supported interfaces.

Example

The following command sets the path failure action for the S5 interface to "signal peer":

```
path-failure s5 signal-peer
```

plmn

Configures the public land mobile network (PLMN) identifier for this S-GW service

Product

S-GW

Privilege

Administrator

Syntax

plmn id mcc *number* **mnc** *number* **[primary]**

no plmn id mcc *number* **mnc** *number*

no

Removes the configured PLMN ID for this S-GW service.

mcc *number*

Configures the Mobile Country Code for this PLMN ID. *number* must be an integer from 100 through 999.

mnc *number*

Configures the Mobile Network Code for this PLMN ID. *number* must be a 2- or 3-digit integer from 00 through 999,

primary

Specifies that this is the primary PLMN ID for this S-GW service.

Usage

Use this command to configure PLMN IDs for this S-GW service

Example

The following command configures a “primary” PLMN ID for this S-GW service with an MCC of *123* and an MNC of *12*:

```
plmn id mcc 123 mnc 12 primary
```

reporting-action

Configures the system to start reporting session events.

Product

S-GW

Privilege

Administrator

Syntax

```
[ no ] reporting-action event-record [ trigger active-idle ]

default reporting-action event-record
```

default

Returns the command to its default setting of disabled.

no

Disables session event reporting.

trigger active-idle

Specifies that the event is only to be reported upon the going from active to idle.

Usage

Use this command to enable the session event reporting feature on the S-GW.

Example

The following command enables event reporting but does not limit it to events triggered by going active to idle:

```
reporting-action event-record
```

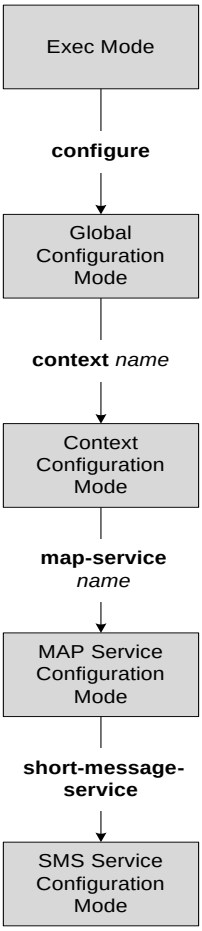
Chapter 257
SMS Service Configuration Mode Commands

The SMS (short message service) Service configuration mode is used to create and manage properties of the SMS Service configuration.

The SGSN uses the SMS Service component to communicate via the Gd interface with a gateway message service controller (GMSC) to send short text messages (up to 140 octets in length) to a mobile (SMS-MT) and/or receive messages from a mobile (SMS-MO) .

When this mode is accessed, the command line will appear similar to

```
[<ctx_name>]asr5000(config-map-service-<map_service_name>-sms-service)#
```



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

cp-data

Enables the SGSN to send and/or receive cp-data (text messages).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

cp-data max-retransmission *retries_num*

default cp-data max-retransmissions

default

This keyword resets the SGSN's max-retransmission to the default number of retries.

max-retransmission *retries_num*

retries_num: enter an integer from 1 to 3.

Usage

Use this command to configure the number of times the SGSN will attempt to retransmit a message.

Example

cp-data max-retransmission *2*

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

mo-message-forwarding-destination

This command defines the SGSN's handling policy for MO (mobile originating) message.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default ] mo-message-forwarding-destination { gmsc-selected-from-imsi | smsc-supplied-by-subscriber }
```

default

Resets the SMS service configuration to the default message forwarding technique.

gmsc-selected-from-imsi

Entering this keyword enables SMS-MO messages to be forwarded on the basis of their IMSI prefix.

smsc-supplied-by-subscriber

Entering this keyword enables SMS-MO messages to be forwarded on the basis of the SMSC (SMS controller) address provided by the subscriber.

Usage

Use this command to define how the mobile originated SMS are to be routed.

Example

```
mo-message-forwarding-destination gmsc-selected-from-imsi
```

smsc-address-restiction-list

Define the list of SMS-C addresses to be screened.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

smsc-address-restriction-list *isdn-no +*

no smsc-address-restriction-list *isdn-no*

no

Delete an SMS-C address (ISDN number) from the list.

isdn-no +

Enter up to 10 ISDN numbers, each up to 15 digits. Put a single space, without a comma, between each ISDN number being added to the list with one command.

Usage

Use this command to identify a list of SMS-C that are to be screened and restricted from receiving forwarded SMS. This list is part of the SMS-C address denial mechanism. For the mechanism to actually function, a second command must be configured, the **smsc-address-restriction-list** command.

Example

Add 3 ISDN numbers to the list of restricted SMS-C addresses.

```
smsc-address-restriction-list 443719933751427 422311198977765
901231445513131
```

Remove an ISDN number from the list of restricted SMS-C addresses.

```
no smsc-address-restriction-list 443719933751427
```

smsc-address-restiction-type

Define the list of SMS-C addresses to be screened.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
smsc-address-restriction-type { mo-mt-sms | mo-sms | mt-sms }

default smsc-address-restriction-type
```

default

Resets the restriction type to the default of both MT and MO types.

mo-mt-sms

Sets the restriction for both types of messages - mobile-originated (MO-SMS) and mobile-terminated (MT-SMS).

mo-sms

Sets the restriction for the mobile-originated (MO-SMS) messages.

mo-mt-sms

Sets the restriction for the mobile-terminated (MT-SMS) messages.

Usage

Use this command to identify the types of messages that are to be denied to the SMS-C identified in the **smsc-address-restriction-type**. Both commands must be configured for the SMS-C address denial mechanism to function.

Example

Restrict MO-SMS messages from being forwarded to the SMS-C listed in the restriction list:

```
smsc-address-restriction-type mo-sms
```

Reset the restriction to both types of messages:

```
default smsc-address-restriction-type
```

smsc-address-selection-prioritization

Define the routing selection priority for the SMSC (short message service center) address to be used for all MO-SMS.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

smsc-address-selection-prioritization from-ms *priority* **imsi-prefix** *priority* **msisdn-prefix** *priority*

default smsc-address-selection-prioritization

from-ms *priority*

Configures a priority for the SMSC address send from the MS.
priority : Value must be a single digit, range 1-3.

imsi-prefix *priority*

Configures a priority for the SMSC address that is based on the IMSI-prefix.
priority : Value must be a single digit, range 1-3.

msisdn-prefix *priority*

Configures a priority for the SMSC address that is based on the MSISDN-prefix.
priority : Value must be a single digit, range 1-3.

default

By including the **default** keyword with the command, the SGSN knows to use the encoded default priorities for SMSC address selection for SMSC routing:

- *from-ms* priority 1,
- *imsi-prefix* priority 2,
- *msisdn-prefix* priority 3.

Usage

Use this command to define SMSC address routing priorities. Priorities must be defined for all parameters, all keywords, but they can be entered in any order. The addresses for the SMSCs are defined with the smsc-routing command.

An operator can use this configuration to prevent subscribers from using unauthorized SMSC addresses, for example, an unauthorized international SMSC.

Example

The keywords can be entered in any order but all keywords must be included in the command:

```
smsc-address-selection-prioritization msisdn-prefix 3 from-ms 1 imsi-prefix 2
```

smsc-routing

This command configures the routing to the short message service center (SMSC).

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] smsc-routing { { any | imsi-starts-with | msisdn-starts-with } { isdn *isdn_number* **| mobile-global-title** *mgt_number* **[max-gt-address-len** *max_gt_length* **] | point-code** *pt_code* **} }**

any

Configures routing according to any IMSI prefix.

imsi-starts-with *IMSI_prefix*

Defines the IMSI prefix. Enter a string of up to 15 digits.

msisdn-starts-with *msisdn_prefix*

Defines the MSISDN prefix. Enter a string of up to 15 digits.

isdn *isdn_number*

Defines the ISDN E.164 number (up to 15 digits) of the SMSC.

mobile-global-title *mgt_number* **[max-gt-address-len** *max_gt_length* **]**

Defines the mobile global title (MGT) E.214 address to be used for IMSI conversion.
Optionally, the maximum length of the GT address can be defined. If the length of the MGT string is greater than the defined max, then the least significant digits will be omitted.
mgt_number is a string of digits, up to 18 digits.
max_gt_address is an integer from 1 to 32.

point-code *pt_code*

Defines the point code for the SMSC. Enter a string of up to 11 digits in SS7 dotted decimal or decimal format

Usage

This command defines the address format (IMSI, point code, mobile global title) and the address for SMSC routing.

Example

Use this command to define routing to the SMSC based on any point code.

```
smsc-routing any point-code 1.222.1
```

timeout

This command defines the SMS service timers.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

timeout { tc1n-timer*time* **| tr1n-timer** *time* **| tr2n timer** *time* **}**

default timeout { tc1n-timer | tr1n-timer | tr2n timer }

default

Resets the configuration to the default value for the specified timer.

tc1n-timer *time*

Configures the TC1N timer in seconds.
time: Must an integer from 1 to 255. The default is 5 seconds.

tr1n-timer *time*

Configures the TR1N timer in seconds.
time: Must an integer from 1 to 255. The default is 30 seconds.

tr2n-timer *time*

Configures the TR2N timer in seconds.
time: Must an integer from 1 to 255. The default is 30 seconds.

Usage

Use this command to set SMS service timers. The command can be repeated to set all of the timers, one-at-a-time.

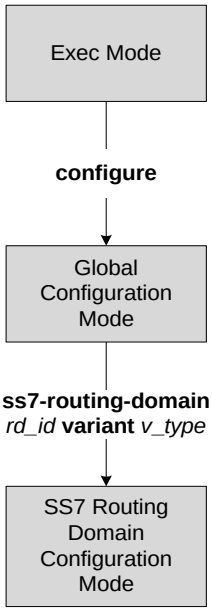
Example

tr1n-timer *25*

Chapter 258
SS7 Routing Domain Configuration Mode Commands

The SS7 Routing Domain configuration mode is used to configure Signaling System 7 (SS7) parameters. For convenience in configuration management, all SS7 parameters have been collected into a proprietary grouping called an *SS7 routing domains*.

`[local]`*`hostname`*`(config-ss7-routing-domain-<`*`ss7rd_id`*`>)#`



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

asp

This command creates or removes an M3UA Application Server Process (ASP) instance and enters the ASP configuration mode. See the *SGSN ASP Configuration Mode* chapter in the *Command Line Interface Reference* for command details.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

asp instance *asp_inst*

no asp instance *asp_inst*

default asp instance *asp_inst* **end-point port**

no

Deletes the ASP instance for the SS7 routing domain configuration.

default

Sets the ASP instance parameters to the end-point port value of 2905.

instance *asp_inst*

Identifies a specific ASP configuration. Up to four ASP instances can be configured for a single SS7 routing domain.
asp_inst : Must be an integer from 1 through 4.

Usage

Use this command to create an ASP instance or enter the ASP configuration mode.

Example

The following command enters the ASP configuration mode for a specific ASP.

```
asp instance 1
```

description

This command defines an alphanumeric string that describes the current SS7 routing domain. This is used for operator reference only.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

description *string*

no description

no

Removes the description string from the current SS7 routing domain configuration.

string

Specifies the alphanumeric string that is stored. Strings with spaces must be enclosed in double-quotes (see the example below).
string: Must be from 1 to 255 alphanumeric characters.

Usage

Use this command to set a description for reference by operators.

Example

The following command sets the description to identify a routing domain for messages transmitted within a national boundary.

```
description "National Service Routing Domain"
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

inbound-asp-identifier validate

This command enables validation of ASP identifiers inbound to the SGSN via routes defined with this SS7 routing domain.

Important: This command is only available in Release 8.1 and higher releases.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
inbound-asp-identifier validate

default inbound-asp-identifier validate

no inbound-asp-identifier validate
```

default

Validates the inbound ASP Id.

no

Disables validation of the inbound ASP Id.

Usage

The standard is to validate the ASP Id. However, in some circumstances it is necessary to skip such validation. For example, if the same ASP Id is assigned to more than one RNC (peer-server).

Example

Use the following command to skip validation of inbound ASP Ids:

```
no inbound-asp-identifier validate
```

Use either of the following commands to enable validation if it has been disabled:

```
default inbound-asp-identifier validate

inbound-asp-identifier validate
```

linkset

This command creates an instance of an MTP3 linkset and enters the Linkset configuration mode. See the Linkset configuration mode chapter for the commands to configure the linkset.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

linkset id *id*

no linkset id *id*

no

Removes the identified linkset definition from the system configuration.

id

This value uniquely identifies a linkset for the specific SS7 routing domain.
id : Must be an integer of 1 to 49.

Usage

This command creates instances of linkset configurations and provides access to the linkset configuration mode.

Example

Use the following command to create the 12th linkset:

```
linkset id 12
```

MTU-size

This command has been deprecated.

peer-server

This command creates a peer-server instance to setup a SIGTRAN peer for sending and receiving M3UA traffic. Completing the command automatically enters the peer- server configuration mode. To define 1 or more (up to 145) peer servers, use the commands documented in the *Peer-Server Configuration Mode* chapter in this reference.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

peer-server id *srvr_id*

no peer-server id *srvr_id*

no

Removes the identified peer-server definition from the system configuration.

srvr_id

srvr_id uniquely identifies a peer-server. The id must be an integer from 1 to 144.

Usage

Use the following command to create a definition for peer-server 2 and enter the configuration mode to configure the communication parameters for peer-server 12.

Example

```
peer-server id 12
```

route

This command configures SS7 routes for the current SS7 routing domain.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

```
route destination-point-code dp_code { linkset id id [ priority pri_value ] | peer-server-id srvr_id }

no route destination-point-code dp_code { linkset id id | peer-server-id srvr_id }
```

no

Removes the SS7 route from the current SS7 routing domain configuration.

destination-point-code *dp_code*

Specifies the SS7 destination point code for this route.
Reminder: the point-code structure must match the variant defined for the SS7 routing domain when the SS7RD was configured in the global configuration mode.

linkset id *id*

This keyword identifies a linkset instance, created and configured with the **linkset** command.
This keyword identifies a linkset instance, created and configured with the **linkset** command.
id : Must be an integer from 1 to 49.

peer-server-id *srvr_id*

This keyword identifies a peer-server configuration instance, created and configured with the **peer-server** command.
srvr_id must be an integer from 1 to 49.

Usage

This command associates the previoiusly configured linksets and peer servers and the destination point codes with a specified SS7 route.

Example

Define a route setting an ITU-type destination point-code address for the linkset Id 12:

```
route destination-point-code 6.211.6 linkset id 12
```

routing-context

Identifies the routing context for this SS7 routing domain.

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

routing-context *value*

default routing-context

default

Resets the local routing context value to the index (instance ID) for this SS7 routing domain.

value

An integer that uniquely identifies the routing context for this SS7 routing domain.
value : Must be integers from 1 to 65535 (for releases 8.0) or 1 to 4294967295 (for releases 8.1 and higher) .

Usage

Use this command to set the routing context IDs for a specific SS7 routing domain configuration.

Example

routing-context *2355*

ssf

This command sets the network indicator in the subservice field for SS7 message signal units (MSUs).

Product

SGSN, HNB-GW

Privilege

Security Administrator, Administrator

Syntax

```
ssf ( international | national | reserved | spare }
```

international

The network indicator identifies the message as international with a point code structure that does not match the national point code structure,

national

The network indicator identifies the messages as having a national point code structure.

reserved

Provides an alternate network indicator for national messages.

spare

Provides an alternate network indicator for international messages.

Usage

In SS7 signaling, the Message Transfer Part (MTP) Level 2 message signal units (MSUs) contain a service information octet (SIO). The SIO field in an MSU contains a 4-bit subservice field (SSF) followed by a 4-bit service indicator. The indicator carried in the message's routing information typically identifies the structure of the point code as a message from within a nation or as a message coming from outside the nation - international. As well, the 4-bit SSF determines the point code structure of the messages transmitted from the SGSN.

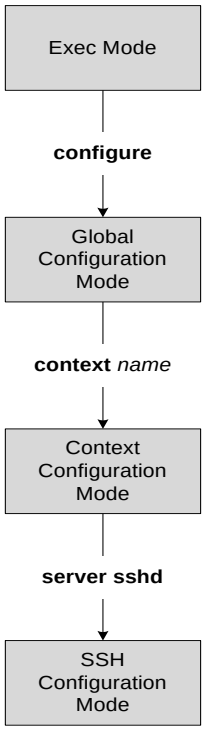
Example

For messages being transmitted within a country, set the indicator to national with the following command.

```
ssf national
```

Chapter 259
SSH Configuration Mode Commands

The Secure Shell Configuration Mode is used to manage the SSH server options for the current context.



Important: You must use the **`ssh generate key`** command in Context Configuration Mode to generate the sshd keys before you can configure the sshd server

authorized-key

Sets or removes a user name having authorized keys for access to the sshd server in the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

authorized-key username *user_name* **host** *host _name* **[type { v2-dsa | v2-rsa }]**

default

Resets the parameter to the default value.

username

Sets a username as having authorized keys for access to the sshd server.

user_name

Specifies the username entered as an alphanumeric string of 1 through 255 characters.

host

Associates an SSH host having the authorization keys for the username.

host_name

Specifies the host name entered as an alphanumeric string of 1 through 255 characters.

[type { v2-dsa | v2-rsa }]

Specifies which type of SSH authorization key will be accepted instead of all key types. The options are: **v2-dsa** (SSHv2 Digital Signature Algorithm), or **v2-rsa** (SSHv2 Rivest, Shamir and Adleman).

Usage

Use this command to set a username with authorized keys for access to the sshd server within the current context.

Example

The following command specifies that username *dbailey* with authorization keys at *sshserver* can access the system with all types of authorization keys:

```
authorized-key username dbailey host sshserver
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

listen

Configures the SSH server in the current context to only listen for connections from the interface with the specified IP address. The default behavior is to listen on all interfaces.

Product

All

Privilege

Security Administrator, Administrator

Syntax

listen *ip_address*

no listen

no

Disable listening for a specific interface address and enable listening on all interfaces.

ip_address

Enables listening only on the interface with the specified IP address. *ip_address* must be entered using IPv4 dotted-decimal notation.

Usage

Use this command to configure the SSH server for the current context to only listen for connections from the interface with the specified IP address. Only one IP address may be set for listening.

Example

The following command specifies that the Server should only listen for connections in the interface with the IP address of *192.168.0.10*:

```
listen 192.168.0.10
```

max servers

Configures the maximum number of SSH servers that can be started within any 60-second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

Product

All

Privilege

Security Administrator, Administrator

Syntax

max servers *number*

number

Default: 40
Specifies the maximum number of servers that can be spawned in any 60-second interval. *number* must be an integer from 1 through 100.

Usage

Set the number of servers to tune the system response as a heavily loaded system may need more servers to support the incoming requests.
The converse would be true as well in that a system can benefit by reducing the number of servers such that telnet services do not cause excessive system impact to other services.

Example

```
max servers 50
```

subsystem

Configures the system to perform file transfers using secure FTP (SFTP) over ssh v2. Administrator users must be configured with the FTP attribute privilege to issue this command.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] subsystem { cli | sftp }
```

no

Disables either the SFTP ssh file transfer method or disables access to the CLI via ssh.

cli

Default: Enabled
Configures the SSH system for the current context to allow access to the CLI.

sftp

Default: Disabled
Enables the SSH system for the current context to perform file transfers using secure FTP (SFTP) over ssh v2.

Usage

Use this command to enable or disable file transfers using secure ftp over an ssh v2 tunnel.
Also use this command to enable or disable access to the CLI over an SSH connection.

Example

The following command enables SFTP for the current context:

```
subsystem sftp
```

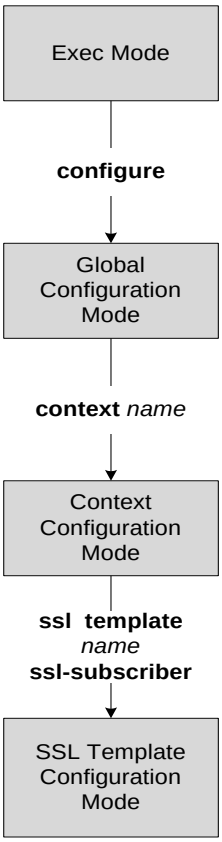
The following command disables access to the CLI through an SSH session for the current context:

```
no subsystem cli
```

Chapter 260
SSL Template Configuration Mode Commands

The SSL Template Configuration Mode is used to configure an SSL cryptographic policy. It includes most of the SSL parameters for cryptographic and authentication algorithms.

A P-CSCF service for SSL access will not function without a configured SSL template. Only one SSL template can be configured per P-CSCF service.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

ca-certificate

Specifies a list of ca-certificates.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

ca-certificate list *name*

list *name*

Specifies the name(s) of ca-certificate(s), which can be an alpha and/or numeric string of 1 to 129 characters.

Usage

Use this command to specify a list of ca-certificates for the SSL template.

Example

The following command specifies the ca-certificate *ca_certificate_1* for the SSL template:

ca-certificate list *ca_certificate_1*

certificate

Used to bind an X.509 trusted certificate to the SSL template.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

certificate *name*

name

Specifies the name of a certificate, which can be an alpha and/or numeric string of 1 to 127 characters.

Usage

Use this command to bind an X.509 certificate to the SSL template.

Example

The following command binds the X.509 certificate *certificate_1* to the SSL template:

certificate *certificate_1*

cipher-suites

Specifies a list of SSL cipher suites.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

cipher-suites list *name*

list *name*

Specifies the name of an SSL cipher suite, which can be an alpha and/or numeric string of 1 to 127 characters.

Usage

Use this command to specify an SSL cipher suite for the SSL template.

Important: Currently, the system supports only one SSL cipher suite per SSL template.

Example

The following command specifies the SSL cipher suite *cipher_suite_1* for the SSL template:

```
cipher-suites list cipher_suite_1
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

version

Specifies the supported version(s) of SSL protocol on the P-CSCF/A-BG.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Syntax

```
version list { tlsv1 }

default version
```

list { tlsv1 }

Specifies the supported version of SSL protocol to be TLS v0.1.

default

Sets the supported version of SSL protocol to its default value of TLS v0.1.

Usage

Use this command to specify the supported version(s) of SSL protocol on the P-CSCF/A-BG. Currently, there is only one supported version of SSL protocol, which is TLS v0.1.

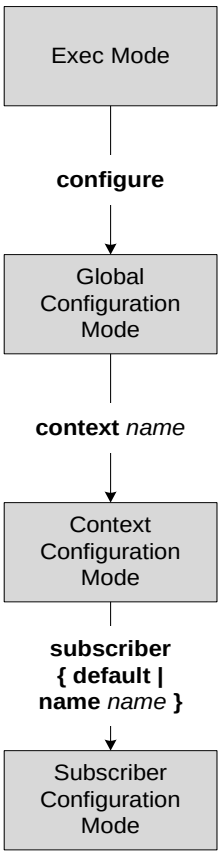
Example

The following command sets the supported version of SSL protocol to TLS v0.1:

```
version list tlsv1
```

Chapter 261
Subscriber Configuration Mode Commands

The Subscriber Configuration Mode is used to create local subscribers as well as to set default subscriber options for the current context.



aaa

This command configures authentication, authorization and accounting (AAA) functionality at the subscriber level.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] aaa { accounting interim { interval-timeout *interval_timeout* **| normal | suppress } | group** *aaa_group_name* **| secondary-group** *aaa_secondary_group_name* **}**

default aaa { accounting interim [interval-timeout] | group | secondary-group }

no aaa { accounting interim [interval-timeout] | group [*aaa_group_name* **] | secondary-group }**

---

default

Configures the default setting for the specified parameter.

- **accounting**: Enables AAA accounting for subscribers.
- **group**: Uses the default AAA group—the one specified at the context level or in the default subscriber profile.
- **secondary-group**: Removes the secondary AAA group from the subscriber configuration.

---

no

- **accounting**: Disables AAA accounting for subscribers.
- **group**: Uses the default AAA group—the one specified at the context level or in the default subscriber profile.
- **secondary-group**: Removes the secondary AAA group from the subscriber configuration.

---

accounting interim { interval-timeout *interval_timeout* **| normal | suppress }**

Specifies when system should send an interim accounting record to the server.

- **interval-timeout**: Specifies the time interval (in seconds) at which to send an interim accounting record.

  interval_timeout must be an integer from 50 through 40000000.

- **normal**: If RADIUS accounting is enabled, send this Acct-Status-Type message when normally required by operation.
- **suppress**: If RADIUS accounting is enabled, suppress the sending of Acct-Status-Type message.

---

group *aaa_group_name*

Specifies the AAA server group for the subscriber for authentication and/or accounting.
aaa_group_name must be an alphanumeric string of 1 through 63 characters.

secondary-group *aaa_secondary_group_name*

Specifies the secondary AAA server group for the subscriber.
aaa_secondary_group_name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure AAA functionality at the subscriber level.
Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual server group for subscribers in that context. Each server group consists of a list of AAA servers for each AAA function (accounting, authentication, charging, etc.).
The AAA secondary server group supports the No-ACK RADIUS Targets feature in conjunction with PDSN/HA for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting the acknowledgement from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start/Interim/Stop) sent to the standard AAA RADIUS server.
If the same AAA group is configured with both the **aaa group** *aaa_group_name* and the **aaa secondary-group** *aaa_group_name* commands, then this configuration will have no effect and secondary accounting will not happen.
The AAA secondary server group configuration takes effect only when used with subscriber accounting-mode set to radius-diameter. The RADIUS accounting triggers for both standard RADIUS accounting and secondary accounting will be taken from the AAA group configured with the **aaa group** *aaa_group_name* command. On the fly change of this configuration is not supported. Any change to the configuration will have effect only for new calls.

Example

The following command applies the AAA server group *star1* to subscribers:

```
aaa group star1
```

access-link ip-fragmentation

Configures IP fragmentation processing over the Access-link.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
access-link ip-fragmentation { normal | df-ignore | df-fragment-and-icmp-notify }
```

df-ignore

Default: Enabled
Ignores the DF (Don’t Fragment) bit setting. Fragments and forwards the packet over the access link.

df-fragment-and-icmp-notify

Default: Disabled
Partially ignores the DF bit. Fragments and forwards the packet, but also returns an ICMP error message to the source of the packet. The number of ICMP errors sent like this is rate-limited to one ICMP error packet per second per session.

normal

Default: Disabled
Normal processing. Drops the packet and sends an ICMP unreachable message to the source of packet. This is the default behavior.

Usage

If the IP packet to be forwarded is larger than the access-link MTU and if the DF (Don't Fragment) bit is set for the packet, then the fragmentation behavior configured by this command is applied. Use this command to fragment packets even if they are larger than the access-link MTU.

Example

Set fragmentation so that the DF bit is ignored and the packet is forwarded anyway by entering the following command:

```
access-link ip-fragmentation df-ignore
```

accounting-mode

Sets the accounting mode for the current local subscriber configuration.

Product

PDSN, HA, ASN-GW, S-GW

Privilege

Administrator

Syntax

```
accounting-mode { flow-based | gtpp [ radius-diameter ] | none | radius-diameter [ gtpp ]
| rf-style }

default accounting-mode
```

default

Sets the type of accounting to be performed for the current local subscriber to the default setting.
Default: **radius-diameter**

flow-based

Diameter flow-based accounting is enabled for the current local subscriber.

gtpp [radius-diameter]

GTPP CDR RADIUS accounting is enabled for the current local subscriber. The **radius-diameter** keyword is available if both GTPP RADIUS and RADIUS-Diameter accounting are to be used.

none

Accounting is disabled for the current local subscriber and no charging records will be generated.

radius-diameter [gtpp]

RADIUS-Diameter accounting is enabled for the current local subscriber. The **gtpp** keyword is available if both GTPP RADIUS and RADIUS-Diameter accounting are to be used.

rf-style

Diameter Rf interface accounting is enabled for the current local subscriber.

Usage

This command specifies which protocol, if any, will be used to provide accounting for PDP contexts accessing the APN profile.
Use this command to enable or disable RADIUS/Diameter accounting for any subscribers that use the current local subscriber configuration.
If the **gtpp** option is used, then GTPP RADIUS is used as configured in the Context Configuration mode or the AAA Server Group Configuration mode and GTPP charging records will be enabled.
If the **radius-diameter** option is used, either the RADIUS or the Diameter protocol is used as configured in the Context Configuration mode or the AAA Server Group Configuration mode.

RADIUS accounting can also be enabled and disabled at the context level with the **aaa accounting** command in the Context Configuration Mode. If RADIUS accounting is enabled at the context level, the accounting-mode command can be used to disable RADIUS accounting for individual local subscriber configurations.
If the accounting mode is set to **rf-style**, then BM will generate accounting records corresponding to AIMS RF.

Example

To disable accounting for the current subscriber, enter the following command:

```
accounting-mode none
```

active-charging bandwidth-policy

Configures the bandwidth policy to be used for the subscriber.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

active-charging bandwidth-policy *bandwidth_policy_name*

{ default | no } active-charging bandwidth-policy

default

Specifies that the default bandwidth policy configured in the rulebase be used for this subscriber.

no

Disables bandwidth control for this subscriber.

active-charging bandwidth-policy *bandwidth_policy_name*

Specifies name of the bandwidth policy.
bandwidth_policy_name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure bandwidth policy to be used for subscribers.

Example

The following command configures a bandwidth policy named *standard* for the subscriber:

```
active-charging bandwidth-policy standard
```

active-charging link-monitor tcp

Enables the TCP link monitoring feature on the Mobile Video Gateway. This command can be configured in either APN Configuration Mode or Subscriber Configuration Mode.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] active-charging link-monitor tcp [ log [ rtt [ histogram | time-series ]
[ bitrate [ histogram | time-series ] ] | bitrate [ histogram | time-series ] [ rtt [
histogram | time-series ] ] ] ][ -noconfirm ]
```

default

Sets TCP link monitoring to its default value, which is the same as **[no]**.

no

Deletes the TCP link monitoring settings and disables TCP link monitoring if previously configured.

active-charging link-monitor tcp

Enables the TCP link monitoring feature on the Mobile Video Gateway. Note that TCP link monitoring is not enabled by default. Also note that when this command is configured without the **log** option, TCP link monitoring is enabled without logging, and the output from TCP link monitoring is only used by the dynamic translating feature.

log [rtt [histogram | time-series] [bitrate [histogram | time-series]] | bitrate [histogram | time-series] [rtt [histogram | time-series]]]

This option enables statistical logging for TCP link monitoring.
The **rtt** option can be used to enable either **histogram** or **time-series** logging for round-trip time (RTT).
Similarly, the **bitrate** option can be used to enable either **histogram** or **time-series** logging for bit rate.
When **rtt** and **bitrate** options are used without additional options, histogram and time-series logging are enabled for round-trip time (RTT) and/or bit rate respectively.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to enable TCP link monitoring on the Mobile Video Gateway.

Examples

The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for both RTT and bit rate:

```
active-charging link-monitor tcp log
```

The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for RTT:

```
active-charging link-monitor tcp log rtt
```

The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT:

```
active-charging link-monitor tcp log rtt histogram
```

The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT and time-series logging enabled for bit rate:

```
active-charging link-monitor tcp log rtt histogram bitrate time-series
```

active-charging rulebase

Specifies the rulebase to be used for this subscriber.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

active-charging rulebase *rulebase_name*

no active-charging rulebase

no

Removes the previously configured rulebase for the subscriber.

active-charging rulebase *rulebase_name*

Specifies name of the ACS rulebase.
rulebase_name must be the name of an ACS rulebase expressed as an alphanumeric string of 1 through 63 characters.

Usage

This command specifies the name of the rulebase for specific subscriber (reals).
If the specified rulebase does not exist in the Active Charging service, the call will be rejected.

Example

The following command configures the ACS rulebase named *rule1* for the subscriber:

```
active-charging rulebase rule1
```

always-on

Once the idle timeout limit is reached, keeps the current subscriber session connected as long as the subscriber is reachable.

Caution: When always-on is enabled, the subscriber must have an idle time-out period configured (default is 0, no time-out). Failure to configure an idle time-out results in a subscriber session that is indefinite.

Two timers and a counter are associated with this feature. Refer to the **timeout** command in this chapter and the **ppp echo-retransmit-timeout msec** and **ppp echo-max-retransmissions num_retries** commands.

Default: Disabled.

Product

PDSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

```
always-on

no always-on
```

always-on

Specifies that the user will remain connected after the idle time expires.

no

Disables **always-on**. The user is disconnected after the idle time expires.

Usage

If this parameter is enabled for a subscriber, when the idle time-out limit is reached the subscribers IP/PPP session remains connected as long as the subscriber is reachable. This is true even if the airlink between the mobile device and the RN (Radio Node) is moved from active to dormant (inactive) status. When the idle timeout limit is reached, the PDSN determines availability using link control protocol (LCP) keepalive messages. A response to these messages indicates that the "always-on" status should be maintained. Failure to respond to a predetermined number of LCP keepalive messages causes the PDSN to tear-down (disconnect) the subscriber session.

Example

Enable always on for the current subscriber by entering the following command:

```
always-on
```

asn-header-compression-rohc

Negotiates Robust Header Compression (ROHC) support for subscriber calls with AAA and WiMAX. This configuration indicates the type of header compression supported and enabled on the ASN.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] asn-header-compression rohc
```

no

Removes or disables the configured identifiers for ROHC in ASN-GW service.

default

The default is *disabled*.

Usage

Network Attached Storage (NAS) uses this configuration to indicate and pack ROHC support the subscriber TLV in the WiMAX-capability attribute in the Access Request. The ROHC header compression is applied only when the ROHC is supported on the ASNGW and ROHC support is indicated by the AAA.

asn nspid

Specifies the network service provider (NSP) associated with a WiMAX subscriber in an ASN-GW service. When configured, the NSP ID is sent in the Access-Request and Accounting messages.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

[no] asn nspid *nsp_id*

no

Removes or disables the configured identifiers for this network service provider in ASN-GW service.

asn nspid *nsp_id*

Specifies the network service provider for this subscriber. This enables the MS to discover all accessible NSPs, and to indicate the NSP selection during connectivity to the ASN.

Usage

Use this command to specify the NSP associated with a subscriber in an ASN-GW service.
nsp_id is three bytes in hexadecimal format. For example: FF-EE-01

Example

The following command specifies the NSP for a subscriber in an ASN service:

```
asn nspid 0F-01-FE
```

asn-pdfid

Configures the identifiers for packet data flow, service data flow, and service profile in an ASN-GW service.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

[no] asn-pdfid *pdf_id* **asn-service-profile-id** *svc_profile_id* **asn-sdfid** *sdf_id*

no

Removes/disables the configured identifiers for this subscriber in ASN-GW service.

asn-pdfid *pdf_id*

Specifies the an unique ASN Packet Data Flow identifier for this subscriber.
pdf_id must be an integer from 1 through 65535.

asn-service-profile-id *svc_profile_id*

Specifies a unique ASN Service Profile Identifier for this subscriber.
svc_profile_id is a Service Profile Identifier configured in the Context Configuration Mode.

asn-sdfid *sdf_id*

Specifies the an unique ASN Service Data Flow identifier for this subscriber.
sdf_id must be an integer from 1 through 65535.

Usage

Use this command to configure subscriber profile for QoS parameters in an ASN-GW service.
A maximum of four QoS profiles can be configured for a subscriber.

Example

The following command configures the QoS profile for a subscriber as PDF id 1, Service Profile id 3, and Service Data Flow id 2:

```
asn-pdfid 1 asn-service-profile-id 3 asn-sdfid 2
```

asn-policy

Configures the identifiers for packet data flow, service data flow, and service profile in an ASN-GW service.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

```
asn-policy [classifiers downlink { strict | loose} | idle-mode { allow | disallow } |
notification-idle-mode {allow | disallow} | notification-handoff { allow | disallow
}auth-only {allow | disallow } | ms-requested-classifiers {allow | dissalow}]

[ default ] asn-policy classifiers downlinkidle-mode
```

no

Removes or disables the configured policy for this subscriber in ASN-GW service.

default

Sets the ASN policy to default for this subscriber.
For downlink traffic classifier default policy is “loos” and for idle mode policy the default action is to allow idle mode operation in an ASN-GW service.

idle-mode

Sets the idle mode policy for this subscriber in an ASN-GW service. If enabled, Interim-Update is sent with the BSID and WiMAX-Idle_Mode Transition as Idle. If disabled, the Interim can be sent when the call is in the idle mode based on the interim timer. At this point, the last known BSID is reported to the RADIUS server.

notification-idle-mode

Default: allow
Use to enable or disable Idle-Mode-Notification capabilities. When you enable this command, when the call moves from active to idle, or idle to active, Accounting Interim is sent.

notification-handoff

Default: allow
If enabled, the Interim-Update is sent with the BSID and SN-Handoff-Indicator as Active Handoff.

allow

Default: enabled
Enables the policy for this subscriber to allow idle mode operation in an ASN-GW service.

disallow

Default: disabled
Enable the policy for this subscriber to disallow idle mode operation in an ASN-GW service.

classifiers downlink

Sets the classifier policy for all service flows coming from HA to FA for this subscriber's matching classifier.

strict

Default: disabled
This option discards all the service flows coming from HA to FA and any other packets not matching to any of the classifiers set for this subscriber.

loose

Default: enabled
This option allows all the service flows coming from HA to FA and any other packet does not matching to any of the classifiers set for this subscriber and sent to the BS/MS over downlink flow

auth-only

Specifies whether the call is Auth only or not.

allow

Enables the policy for this subscriber to allow auth-only in an ASN-GW service.

disallow

Default
Disables the policy for this subscriber to allow auth-only in an ASN-GW service.

ms-requested classifiers

Default: allow
By default ASNGW allows dynamic addition of classifiers by the MS during MS-initiated service flow creation or modification.

Usage

Use this command to configure subscriber policy to allow/disallow the idle mode operation or the downlink traffic flow for a subscriber in an ASN-GW service.
For authentication configuration, the ASN-GW supports the Initial Network Entry (INE) for Ethernet CS calls. The base station supports Ethernet CS traffic to the network. The INE procedure includes the Authentication of the service flows and IP-Address allocation through DHCP. Authentication is based on the Extensible Authentication Protocol (EAP).
This command allows MS to transition to idle mode with an ASN-GW.

Example

The following command configures the policy to allow the idle mode for an MS with an ASN-GW:

```
default asn-policy idle-mode
```

authorized-flow-profile-id

When a profile ID is requested by the Mobile Node (MN), this command sets the value that is authorized by the Access Gateway (AGW).

Product

PDSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

authorized-flow-profile-id *profile_id* **direction { bidirectional | forward | reverse }**

no authorized-flow-profile-id *profile_id*

no

Removes the existing profile ID setting specified by *profile_id*. *profile_id* must be an integer from 0 through 65535.

authorized-flow-profile-id *profile_id*

The profile ID number that is authorized for the current subscriber. *profile_id* must be an integer from 0 through 65535.

direction { bidirectional | forward | reverse }

This specifies in which data direction the profile ID should be applied.

- **bidirectional**: This profile ID pertains to both the forward and reverse directions.
- **forward**: This profile ID pertains to data going to the MN.
- **reverse**: This profile ID pertains to data coming from the MN.

Usage

Use this command to set the profile ID that the AGW will authorize for a subscriber.

Example

Set the profile ID for both directions to 3 for the current subscriber by entering the following command:

```
authorized-flow-profile-id 3 direction bidirectional
```

content-filtering category

Enables or disables the specified preconfigured Category Policy Identifier for policy-based Content Filtering support to the subscriber.

Product

CF

Privilege

Security Administrator, Administrator

Syntax

content-filtering category policy-id *cf_policy_id*

no content-filtering category policy-id

no

Disables the configured category policy ID for content filtering support to the subscriber. This is the default setting.

content-filtering category policy-id *cf_policy_id*

Applies the content filtering category policy ID, configured in ACS Configuration Mode, to this subscriber.
cf_policy_id must be a category policy ID expressed as an integer from 1 through 4294967295.
If the specified category policy ID is not configured in the ACS Configuration Mode, all packets will be passed regardless of the categories determined for such packets.

Important: Category Policy ID configured through this mode overrides the Category Policy ID configured using the **content-filtering category policy-id** command in the ACS Rulebase Configuration Mode.

Usage

Use this command to enter the Content Filtering Policy Configuration Mode and enable or disable the Content Filtering Category Policy ID for a subscriber.

Important: If Content Filtering Category Policy ID is not specified here, the similar command in the ACS Rulebase Configuration Mode determines the policy.

Up to 64 different policy identifier can be defined in a Content Filtering support service.

Example

The following command enters the Content filtering Policy Configuration Mode and enables the Category Policy ID *101* for Content Filtering support:

```
content-filtering category policy-id 101
```

credit-control-group

Configures the credit-control group for this subscriber.

Product

All

Privilege

Security Administrator, Administrator

Syntax

credit-control-group *cc_group_name*

no credit-control-group

no

Removes the credit-control group from the subscriber configuration, if configured.

credit-control-group *cc_group_name*

Specifies name of the credit-control group.
cc_group_name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the credit-control group for the subscriber.

Example

The following command configures the credit-control group named *test12* for the subscriber:

```
credit-control-group test12
```

credit-control-service

Configures the credit-control service for this subscriber.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] credit-control-service *cc_service_name*

no

Disables the credit-control service, if configured.

credit-control-service *cc_service_name*

Specifies the name of the credit-control service.
cc_service_name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the credit-control service for subscribers.

Example

The following command configures the credit-control service named *test12* for the subscriber:

```
credit-control-service test12
```

cscf core-service

CSCF/A-BG core service that maps to the current domain.

Product

SCM (CSCF, A-BG)

Privilege

Security Administrator, Administrator

Syntax

cscf core-service name *name*

no cscf core-service

cscf core-service name *name*

Specifies the name of the CSCF/A-BG core service.
name must be an alphanumeric string of 1 through 63 characters.

no cscf core-service

Removes the CSCF/A-BG core service from the domain.

Usage

Use this command to map a CSCF/A-BG core service to the current domain.

Example

The following command creates a CSCF core service named *cs1*:

```
cscf core-service name cs1
```

The following command removes the CSCF core service from this domain:

```
no cscf core-service
```

cscf county-name

Assigns a Last Routing Option (LRO) profile county name to the subscriber for finding the correct Public Safety Answering Point (PSAP) during emergency calls.

Product

SCM (S-CSCF)

Privilege

Security Administrator, Administrator

Syntax

[no] cscf county-name *name*

cscf county-name *name*

Specifies the LRO profile county name of the subscriber.
name must be an existing LRO profile county name expressed as an alphanumeric string of 1 through 127 characters.

no

Removes the LRO profile county name from the subscriber.

Usage

Use this command to assign an LRO profile county name to the subscriber.

Example

The following command assigns county name *norfolk* to the subscriber:

```
cscf county-name norfolk
```

The following command removes county name *norfolk* from the subscriber:

```
no cscf county-name norfolk
```

cscf nat-applicable

Indicates if NAT (Network Address Translation) processing is required for this domain.

Product

SCM (CSCF/A-SBC)

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] cscf nat-applicable
```

no

Disables NAT processing for this domain.

cscf nat-applicable

Enables NAT processing for this domain.

Usage

Use this command to indicate whether NAT processing is required for this domain.

Example

The following command indicates NAT processing is required for this domain:

```
cscf nat-applicable
```

The following command disables NAT processing for this domain:

```
no cscf nat-applicable
```

cscf private-user-id

Assigns a private user identity to the subscriber.

Product

SCM (P-CSCF, S-CSCF, SIP Proxy)

Privilege

Security Administrator, Administrator

Syntax

[no] cscf private-user-id *user_id*

no

Removed the private user identity of the subscriber.

cscf private-user-id *user_id*

Specifies the private user identity of the subscriber.
user_id must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to assign a private user identity to the subscriber.

Example

The following command assigns a private user identity named *user007* to the subscriber:

```
cscf private-user-id user007
```

The following command removes private user identity named *user007* from the subscriber:

```
no cscf private-user-id user007
```

cscf session-template

Assigns a CSCF session template to the subscriber profile.

Product

SCM (P-CSCF, S-CSCF, SIP Proxy)

Privilege

Security Administrator, Administrator

Syntax

cscf session-template name *name*

no cscf session-template

cscf session-template name *name*

Specifies the name of the CSCF session template.
name must be an existing CSCF session template name expressed as an alphanumeric string of 1 through 79 characters.

no cscf session-template

Removes the assignment of a session template to the subscriber profile.

Usage

Use this command to bind a CSCF session template to a subscriber profile.

Example

The following command assigns a CSCF session template named *template4* to the subscriber profile:

```
cscf session-template name template4
```

The following command removes the assignment of a session template to the subscriber profile:

```
no cscf session-template
```

data-tunneling ignore df-bit

Controls the handling of the DF (Don't Fragment) bit present in the user IPv4/IPv6 packet for GRE, IP-in-IP tunneling used for the MIP data path. If this feature is enabled, and fragmentation is required for the tunneled user IPv4/IPv6 packet, then the DF bit is ignored and the packet is fragmented. Also the DF bit is not copied to the outer header. Default is enabled.

Product

PDSN, HA, FA, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

```
data-tunneling ignore df-bit

no data-tunneling ignore df-bit
```

no

Disables this option. The DF bit in the tunneled IP packet header is not ignored during tunneling.

data-tunneling ignore df-bit

Ignores the DF bit in the tunneled IP packet header.

Usage

Use this command to configure a user so that during Mobile IP tunneling the DF bit is not ignored and packets are not fragmented.

Example

To disable fragmentation of a subscribers packets over a MIP tunnel even when the DF bit is present, enter the following command:

```
no data-tunneling ignore df-bit
```

dcca origin host

This command is obsolete. Refer to the **dcca origin endpoint** command.

dcca origin endpoint

This command is obsolete. To configure the Diameter Credit Control Origin Endpoint, in the Credit Control Configuration Mode, use the **diameter origin endpoint** command.

dcca peer-select

Specifies the Diameter credit control primary and secondary peer for credit control.

Product

ACS

Privilege

Security Administrator, Administrator

Syntax

dcca peer-select peer *host_name* **[realm** *realm_name* **] [secondary-peer** *host_name* **[realm** *realm_name* **]]**

no dcca peer-select

no

Removes the previously configured Diameter credit control peer selection.

peer *host_name*

Specifies a unique name for the peer. *peer_name* must be an alphanumeric string of 1 through 63 characters that allows punctuation marks.

secondary-peer *host_name*

Specifies a back-up host that is used for fail-over processing. When the route-table does not find an available route, the secondary host performs a fail-over processing. *host_name* must be an alphanumeric string of 1 through 63 characters that allows punctuation marks.

realm *realm_name*

The *realm_name* must be an alphanumeric string of 1 through 63 characters that allows punctuation marks. The realm may typically be a company or service name.

Usage

Use this command to select a Diameter credit control peer and realm.

WARNING: This configuration completely overrides all instances of **diameter peer-select** that have been configured with in the Credit Control Configuration Mode for an Active Charging service.

Example

The following command selects a Diameter credit control peer named *test* and a realm of *companyx*:

```
dcca peer-select peer test realm companyx
```

default

Restores the default value for the option specified for the current subscriber.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
default { access-link ip-fragmentation | accounting-mode | data-tunneling ignore df-bit |
idle-timeout-activity dormant-downlink-data | inter-pdsn-handoff | ip { alloc-method |
allowed-dscp | header-compression | hide-service-address | multicast discard | qos-dscp |
source-validation } | loadbalanace-tunnel-peers | long-duration-action | mobile-ip {
home-agent | mn-aaa-removal-indication | mn-ha-hash-algorithm | reverse-tunnel |
security-level | send { dns-address | terminal-verification } } | permission | ppp {
always-on-vse-packet | data-compression { mode | protocols } | keepalive | min-
compression-size | mtu } | radius accounting interim interval-timeout | timeout {
absolute | idle } }
```

access-link ip-fragmentation

Sets the method for fragmenting packets over the MN access link to its default of normal. Drop the packet and send ICMP unreachable to the source of packet.

accounting-mode

Enables Radius accounting for the current local subscriber configuration.

data-tunneling ignore df-bit

Sets this option to the default behavior, which is to send an *ICMP unreachable - need to frag* message back to the sender and drop the packet, in the case that fragmentation is required but the DF bit is set.

idle-timeout-activity dormant-downlink-data

Sets this option to the default behavior. When downlink data packets are transmitted to the Mobile node and the session is in dormant mode the session idle timer is reset.

inter-pdsn-handoff

During a handoff from one PDSN to another, if the Mobile requests an IP address of 0.0.0.0 or a mismatched IP address the PDSN will not disconnect the session immediately. The PDSN tries to assign the proposed address of the session in the IPCP configuration NAK.

ip { | allowed-dscp | dhcp-relay | header-compression | hide-service-address | multicast discard | qos-dscp | source-validation | user-datagram-tos copy }

allowed-dscp: resets the allowed DSCP parameters to the system defaults: class none, max-class be.
hide-service-address: specifies the default setting for hide the ip-address of the service from the subscriber. Default is Disabled

dhcp-relay: Configured with the DHCP server address during MS authentication. The AAA server sends the address of the DHCP server in the Access-Accept message. The DHCP relay uses this address to relay the DHCP messages from the MS to the DHCP server.
multicast discard: Configures the default multicast settings which is to discard PDUs
qos-dscp: Sets the quality of service setting to the system default.
source-validation: Specifies the default IP source validation. Default is Enabled.
user-datagram-tos copy: Disables copying of the IP TOS octet value to all tunnel encapsulation IP headers.

---

loadbalance-tunnel-peers

Sets the tunnel load balancing algorithm to the system default.

---

long-duration-action

Sets the action that is taken when the long duration timer expires to the default: detection.

---

mobile-ip { home-agent | mn-aaa-removal-indication | mn-ha-hash-algorithm | reverse-tunnel | security-level | send { dns-address | terminal-verification } }

allow-aaa-address-assignment: Disables the FA from accepting a home address assigned by an AAA server.
home-agent: Sets home agent IP address to its default of 0.0.0.0.
match-aaa-assigned-address: Disables the FA validating the home address in the RRQ against the one assigned by AAA server.
mn-aaa-removal-indication: Sets this parameter to its default of disabled.
mn-ha-hash-algorithm: Sets the encryption algorithm to the default of hmac-md5.
reverse-tunnel: Sets this parameter to its default of enabled.
security-level: Sets this parameter to its default of none.
send dns-address: Disables the HA from sending the DNS address NVSE in the RRP.
send terminal-verification: Disables the FA from sending the terminal verification NVSE in the RRQ.

---

permission

Restores the subscriber's service usage defaults.

---

ppp { always-on-vse-packet | data-compression { mode | protocols } | ip-header-compression negotiation | keepalive | min-compression-size | mtu }

Sets the point-to-point protocol option defaults.
always-on-vse-packet: Re-enables the PDSN to send special 3GPP2 VSE PPP packets to the Mobile Node with a max inactivity timer value for always on sessions. This configuration is applicable only for PDSNsessions.
data-compression { **mode** | **protocols** }: restores the default value for either the data compression **mode** or compression **protocols** as follows:

- mode stateless
- all protocols enabled

ip-header-compression negotiation: Sets the IP header compressions negotiation to the system default: force.
keepalive: sets the subscriber's PPP keep alive option to the system default: 30 seconds.
min-compression-size: Restores the PPP minimum packet size for compression: 128 octets.

mtu: Sets the maximum message transfer unit packet size to the system default: 1500 octets.

radius accounting interim interval-timeout

Disables the RADIUS accounting interim interval for the current subscriber.

timeout [absolute | idle | long-duration]

When a keyword is entered, this command resets the specified timeout to the system default: 0. When no keyword is specified, all timeouts are reset to the system defaults: 0.

Usage

Use this keyword to reset subscriber data to the system defaults. This is useful in setting the subscriber back to the basic values to possibly aid in trouble shooting or tuning a subscriber's access and options.

Example

```
default ip qos-dscp

default permission

default data-compression mode
```

dns

Configures the domain name servers for the current subscriber.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] dns { primary | secondary } *ip_address*

no

Indicates the IP address is to be removed as either a primary or secondary domain name server.

dns primary | secondary

dns primary: Updates the primary domain name server for the subscriber.
dns secondary: Updates the secondary domain name server for the subscriber.

ip_address

Specifies the IP address of the domain name server using IPv4 dotted-decimal notation.

Usage

Set the subscriber DNS server lists as not all users will have the same set of servers.

Example

```
dns primary 10.2.3.4

no dns primary 10.2.3.4

dns secondary 10.2.5.6

no dns secondary 10.2.5.6
```

eap

Specifies the lifetime for a master session key (MSK) for extensible authentication protocol (EAP) authentication.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

[default] eap msk-lifetime *dur*

default

Sets the lifetime duration to default value of 3600 seconds for master session key.

msk-lifetime *dur*

Specifies the lifetime duration (in seconds) on Master Session Key (MSK) in seconds for a WiMAX subscriber EAP authentication.
dur is an integer from 60 through 65535.

Usage

This command is used to set the lifetime for MSK in EAP authentication for WiMAX subscriber.

Example

The following command sets the lifetime for MSK key to *4800* seconds for a WiMAX subscriber through EAP authentication:

```
eap msk-lifetime 4800
```

encrypted password

Designates use of password encryption.

Product

All

Privilege

Security Administrator, Administrator

Syntax

encrypted password *password*

encrypted password *password*

password is the encrypted password and must be an alphanumeric string of 1 through 132 characters.

Usage

This command is normally used only inside configuration files.

Example

The following command sets an encrypted password of *qsdf12d4*:

```
encrypted password qsdf12d4
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

external-inline-server

This is a restricted command.

firewall policy

Important: This command is only available in StarOS 8.0. In StarOS 8.1 and later releases, this configuration is available in the ACS Rulebase Configuration Mode.

This command enables or disables Stateful Firewall support for the subscriber.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
firewall policy firewall-required

{ default | no } firewall policy
```

no

Disables Stateful Firewall support for this subscriber.

default

Configures the default setting for Stateful Firewall support.
Default: Disabled

firewall-required

Enables Stateful Firewall support for this subscriber.

Usage

Use this command to enable or disable Stateful Firewall support for this subscriber.

Important: Unless Stateful Firewall support for this subscriber is enabled using this command, firewall processing for this subscriber is disabled.

Important: If firewall is enabled, and the rulebase has no firewall configuration, Stateful Firewall will cause all packets to be discarded.

Example

The following command enables Stateful Firewall support for this subscriber:

```
firewall policy firewall-required
```

The following command disables Stateful Firewall support for this subscriber:

```
no firewall policy
```

fw-and-nat policy

Important: This command is only available in StarOS 8.1. This customer-specific command must be used to configure the Policy-based Firewall-and-NAT feature.

Product

FW, NAT

Privilege

Security Administrator, Administrator

Syntax

fw-and-nat policy *fw_nat_policy*

{ default | no } fw-and-nat policy

default

Specifies that the default Firewall-and-NAT policy configured in the rulebase be used for the subscriber.

no

Disables Firewall and NAT processing for the subscriber.

fw_nat_policy

Specifies the Firewall-and-NAT policy for the subscriber.
fw_nat_policy must be an alphanumeric string of 1 through 63 characters. Note that this policy will override the **default Firewall-and-NAT policy** configured in the ACS rulebase.

Usage

Use this command to configure the Firewall-and-NAT policy for subscribers. Note that the policy configured in the subscriber mode will override the default policy configured in the ACS rulebase. If a policy is not configured in the subscriber mode, the default policy configured in the ACS rulebase will be applied.

Example

The following command configures a Firewall-and-NAT policy named *standard* for the subscriber:

```
fw-and-nat policy standard
```

idle-timeout-activity

Defines whether downlink (towards Mobile Node) data packets transmitted when the session is dormant are treated as activity for the idle-timer (inactivity timer).

By default, downlink data transmitted over a dormant session restarts the idle-timer for that session; it is treated as activity for the session.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] idle-timeout-activity dormant-downlink-data
```

no

Dormant mode downlink data is not treated as activity for the session idle-timer. The session idle timer is not reset.

idle-timeout-activity dormant-downlink-data

Treats dormant mode downlink data as activity for the session idle-timer. The session idle timer is reset.

Usage

Use this command to disable or re-enable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode.

Example

Use the following command to disable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode:

```
no idle-timeout-activity dormant-downlink-data
```

Use the following command to re-enable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode:

```
idle-timeout-activity dormant-downlink-data
```

ims application-manager

Specifies the IP Multimedia Subsystem (IMS) application manager for the subscriber.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

[no] ims application-manager { domain-name *domain-name* **| ipv4-address** *ipv4_address* **}**

no

Disables the IMS application manager for this subscriber.

ims application-manager

Enables the IMS application manager for this subscriber.

domain-name *domain-name*

Specifies the domain name of the application manager.
domain-name must be an alphanumeric string of 1 through 63 characters.

ipv4-address *ipv4_address*

Specifies the IP address of the application manager using IPv4 dotted-decimal notation.

Usage

The IMS application manager address is returned by HA to MN in DHCP Ack when it receives the DHCP inform from an AIMS subscriber.

Example

```
ims application-manager domain-name domain23ims application-manager ipv4-
address 192.168.23.1
```

ims-auth-service

Enables IP Multimedia Subsystem (IMS) authorization support for subscriber. The specified IMSA service will be used for performing IMS authorization and flow-based charging procedures.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

[default | no] ims-auth-service *auth_svc_name*

default

Configures default setting.
Default: Disabled or as specified at the context or network access service level or in subscriber template.

no

Removes the specified IMS authorization service from the subscriber configuration.

ims-auth-service *auth_svc_name*

Specifies name of the IMS authorization service.
auth_svc_name must be an alphanumeric string of 1 through 63 characters preconfigured within the same context of this subscriber.

Usage

This feature provides the IMS authorization service configuration for Gx interface in IMS service node.

Example

Following command applies a previously configured IMS authorization service named *ims_interface1* to a subscriber within the specific context.

```
ims-auth-service ims_interface1
```

inter-pdsn-handoff

Configure the system to force the MN to use its assigned IP address during Internet Protocol Control Protocol (IPCP) negotiations resulting from inter-PDSN handoffs.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] inter-pdsn-handoff require ip-address
```

no

Disables the rejecting of sessions when the MN uses a non-allocated IP address during IPCP re-negotiations.

inter-pdsn-handoff require ip-address

Rejects sessions when the MN uses a non-allocated IP address during IPCP re-negotiations.

Usage

This command is used to configure the system to reject sessions that are re-negotiating IPCP after an inter-PDSN handoff if the IP address they propose does not match the one initially provided by the PDSN. The session would be rejected even if the proposed address was 0.0.0.0.
If this parameter is disabled, the PDSN will attempt to re-assign the IP address initially provided.

Example

To set the PDSN to not allow a mismatched IP address during a PDSN to PDSN handoff of a MIP call, use the following command:

```
inter-pdsn-handoff require ip-address
```

To set the PDSN so that it will not disconnect the session immediately, if the Mobile requests an IP address of 0.0.0.0 or a mismatched IP address after inter-pdsn handoff, use the following command:

```
no inter-pdsn-handoff require ip-address
```

ip access-group

Configures IP access group for the current subscriber.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] ip access-group *group_name* **[in | out]**

no

Indicates the access group specified is to be cleared from the subscribers configuration.

ip access-group *group_name*

Specifies the name of the IPv4/IPv6 access group. *acl_group_name* is a configured ACL group expressed as an alphanumeric string of 1 through 79 characters.

in | out

Default: both (in and out)
Specifies the access-group as either inbound or outbound by the keywords **in** and **out**, respectively. If neither of these key words is specified, the command associates the *group_name* access group with the current subscriber for both inbound and outbound access.

Usage

Set the subscriber access group to manage the access control for subscribers as a logical group.

Example

The following command associates the *sampleGroup* access group with the current subscriber for both inbound and outbound access:

```
ip access-group sampleGroup
```

The following removes the outbound access group flag for *sampleGroup*:

```
no ip access-group sampleGroup out
```

ip address

Configures a static IPv4 address for use by the subscriber.

Product

PDSN, GGSN, HA, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

[no] ip address *ip_address netmask*

no

Removes a previously configured IP address assignment.

ip address *ip_address*

Specifies the IP address assigned to the subscriber using IPv4 dotted-decimal notation.

netmask

The subnet mask that corresponds to the assigned IPv4 address.

Usage

Use this command to assign a static IPv4 address to the subscriber. This address will be used each time the subscriber establishes data sessions.

Example

The following command configures a static IP address of *192.168.1.15* with a subnet mask of *255.255.255.0* to the subscriber:

```
ip address 192.168.1.15 255.255.255.0
```

ip address pool

Configures IP address pool properties for the subscriber.

Product

PDSN, GGSN, HA, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

[no] ip address pool name *pool_name*

no

Removes a previously configured static address.

ip address pool name *pool_name*

Specifies the IP address pool or IP address pool group from which the subscribers IP address is assigned. *pool_name* must be the name of an existing IP pool or IP pool group expressed as an alphanumeric string of 1 through 31 characters.

Usage

Use this command to specify the name of an IP address pool configured on the system from which IP addresses are to be dynamically assigned to sessions from this subscriber.
This command can be issued multiple times to specify multiple address pools for the subscriber. If multiple pools are specified, addresses are assigned for subscriber sessions from the pools based on the order in which the pools were configured.
If an address cannot be provided from the first-specified pool for whatever reason, the system attempts to assign an address from the second-specified pool, and so on. This operation is independent of the priorities configured for the pools. For example, if pool1 was specified for the subscriber first, and pool2 second, the system always attempts to assign addresses from pool1. If an address can not be assigned from pool1 (i.e. all addresses are in use), the system then attempts to assign an address from pool2.

Example

The following command configures the subscriber to receive IP addresses from an IP address pool named *public1*:

```
ip address pool name public1
```

ip address secondary-pool

Configures secondary IP address pool properties for the subscriber to provide multiple IP host configuration behind one WiMAX Customer Premise Equipment (CPE).

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

[no] ip address secondary-pool name *aux_pool_name*

no

Removes a previously configured auxiliary pool named *aux_pool_name* for multiple host support in ASN-GW service.

ip address secondary-pool name *aux_pool_name*

Specifies the secondary/auxiliary IP address pool or IP address pool group from which the IP address is assigned to host behind a WiMAX CPE having primary IP address.
pool_name must be the name of an existing IP pool or IP pool group expressed as an alphanumeric string of 1 through 31 characters.

Usage

Use this command to specify the name of an IP address pool configured on the system from which IP addresses are to be dynamically assigned to host behind a WiMAX CPE for multiple host session support. This command designates the IP address to secondary hosts from locally configured secondary IP address pool. To enable multiple host support behind a WiMAX CPE and configure maximum number of supported hosts use **secondary-ip-host** command in ASN Gateway Service Configuration mode.

Example

The following command configures the subscriber to receive IP addresses from a secondary IP address pool named *auxiliary1* for secondary hosts behind the WiMAX CPE:

```
ip address secondary-pool name auxiliary1
```

ip allowed-dscp

Sets the Quality of Service (QoS) Differentiated Services (DiffServ) marking that a subscriber session is allowed. The DSCP is disabled by default.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip allowed-dscp class *class* **max-class maxclass [rt-marking** *marking* **]**

no ip allowed-dscp class

---

no

Resets the parameters to the defaults: class none, max-class **be**. This indicates that all packets are let through without any dscp checking

---

ip allowed-dscp class *class*

Specifies the Differentiated Services Codepoint (DSCP) class with which the subscriber session may mark its packets. If the subscriber sessions packets request a code point class higher than the code point class specified, the PDSN service re-marks the packets with the QOS-DSCP value specified by the **ip qos-dscp** command.
Default: none
class must be one of the following;
a: allow packets with AF DSCPs
e: allow packets with EF DSCP
o: allow packets for experimental or local use
ae: allow packets with AF and EF DSCPs
ao: allow packets with AF DSCPs or packets for experimental or local use
eo: allow packets with EF DSCPs or packets for experimental or local use
aeo: allow packets with AF or EF DSCPs or packets for experimental or local use
none: allow only the **be** and **sc1** through **sc7** code points

---

max-class *maxclass*

This parameter specifies the maximum code point with which a subscriber session may mark its packets. The subscriber sessions packets must be marked with a code point equal to or less than the code point specified. If the subscriber sessions packets request a code point higher than the code point specified, the PDSN service re-marks the packets with the QOS-DSCP value specified by the lower of the max-class and the **ip qos-dscp** command.
The list below identifies the code points from lowest to highest precedence. For example, if the **maxclass** is set to af22, that becomes the maximum code point that the subscriber session may mark it's packets with and only **be, af13, af12, af11,af23**, and **af22** are allowed. If a subscriber session marks its packets with anything after af22 in this list, the PDSN service re-marks the packets with the QOS-DSCP value specified by the lower of the maxclass and the **ip qos-dscp** command.
If class is set to none only the be and sc1 through sc7 codepoints are allowed. For example; if **class** is set to none and you set **max-class** to **sc1**, only the **sc1** and **be** codepoints are allowed.
Default: **be**

maxclass must be one of the following;
be: best effort forwarding
af13: assured Forwarding 13
af12: assured Forwarding 12
af11: assured Forwarding 11
af23: assured Forwarding 23
af22: assured Forwarding 22
af21: assured Forwarding 21
af31: assured Forwarding 31
af32: assured Forwarding 32
af33: assured Forwarding 33
af41: assured Forwarding 41
af42: assured Forwarding 42
af43: assured Forwarding 43
ef: expedited forwarding
sc1: selector class 1
sc2: selector class 2
sc3: selector class 3
sc4: selector class 4
sc5: selector class 5
sc6: selector class 6
sc7: selector class 7

---

rt-marking *marking*

This parameter is used for Mobile IP (MIP) reverse tunnels. When MIP session packets do not have a DSCP marking, the Foreign Agent (FA) marks the packets with the value specified by **rt-marking** *marking*.
If MIP sessions packets have a DSCP marking, the marking is subjected to the conformance rules for the values of class and max-class; the final DSCP marking is then copied from the inner IP header to the outer IP header.
Default: **be**
marking must be one of the following;
be: best effort forwarding
af11: assured Forwarding 11
af12: assured Forwarding 12
af13: assured Forwarding 13
af21: assured Forwarding 21
af22: assured Forwarding 22
af23: assured Forwarding 23
af31: assured Forwarding 31
af32: assured Forwarding 32
af33: assured Forwarding 33
af41: assured Forwarding 41
af42: assured Forwarding 42
af43: assured Forwarding 43
ef: expedited forwarding
sc1: selector class 1
sc2: selector class 2
sc3: selector class 3
sc4: selector class 4
sc5: selector class 5
sc6: selector class 6

sc7: selector class 7

Usage

Use this command to configure Quality of Service (QoS) for a subscriber session to allow a Differentiated Services (DiffServ) Code Point (DSCP) marker in the header of each IP packet that prompts network routers to apply differentiated grades of service to various packet streams.
This command uses **class** and type of marker (**rt-marking** for reverse tunnels) for configuration with **max-class** maximum code point that a subscriber session may mark its packets with.

Example

The following command will allow *o* packets for experimental or local use with best effort forwarding *be*:

```
ip allowed-dscp class o max-class be
```

ip context-name

Configures the context to which the subscriber is assigned upon authentication. The assigned context is considered the destination context that provides the configuration options for the services the subscriber is allowed to access.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] ip context-name *name*

no

Removes the current assigned context from the subscriber's data.

ip context-name *name*

Specifies the name of the context to assign the subscriber to once authenticated. *name* must be an alphanumeric string of 1 trough 79 characters.

Usage

Set the subscriber IP context to a common context when all subscribers from one or more contexts will use the same egress context.

Example

```
ip context-name sampleName

no ip context-name sampleName
```

ip header-compression

Configures the IP packet header compression options for the current subscriber. Although this command configures IP header compression algorithms, the Internet Protocol Control Protocol (IPCP) negotiations determine when the header compression algorithm is applied.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
ip header-compression { rohc [ any [ mode { optimistic | reliable | unidirectional } ] |
cid-mode { { large | small } [ marked-flows-only | max-cid | max-hdr value | mrru value ]
} | marked flows-only | max-hdr value | mrru value | downlink | uplink ] | vj } +

[ default | no ] ip header-compression
```

default

Restores this command's default setting to the Van Jacobsen (VJ) header compression algorithm.

no

Disables all IP header compression.

ip header-compression { rohc [any [mode { optimistic | reliable | unidirectional }] | cid-mode { { large | small } [marked-flows-only | max-cid | max-hdr *value* | mrru *value*] } } | marked flows-only | max-hdr *value* | mrru *value* | downlink | uplink] | vj }

Specifies that the Robust Header Compression (ROHC) algorithms is used for data.

Important: ROHC is only supported for use with the PDSN.

any: Apply ROHC header compression in both the uplink and downlink directions.
mode { optimistic | reliable | unidirectional }:

- **optimistic**: Sets the ROHC mode to Bidirectional Optimistic mode (O-mode). In this mode packets are sent in both directions. A feedback channel is used to send error recovery requests and (optionally) acknowledgments of significant context updates from decompressor to compressor. Periodic refreshes are not used in the Bidirectional Optimistic mode.
- **reliable**: Sets the ROHC mode to Bidirectional Reliable mode (R-mode). This mode applies an intensive usage of a feedback channel and a strict logic at both the compressor and the decompressor that prevents loss of context synchronization between the compressor and the decompressor. Feedback is sent to acknowledge all context updates, including updates of the sequence number field.
- **unidirectional**: Sets the ROHC mode to Unidirectional mode (U-mode). With this mode packets are sent in one direction only, from the compressor to the decompressor. This mode therefore makes ROHC usable over links where a return path from the decompressor to the compressor is unavailable or undesirable.

cid-mode { { large | small } [marked-flows-only | dm | max-hdr *value* **| mrru** *value* **] }**: Specifies the ROHC packet type to be used.

- **large | small [marked-flows-only | max-cid | max-hdr** *value* **| mrru** *value* **]**: Defines the ROHC packet type as large or small and optionally sets the following parameters for the packet type selected:
- **marked-flows-only**: Specifies that ROHC is to be applied only to marked flows.
- **max-cid** *integer*: Default: 0 The highest context ID number to be used by the compressor. *integer* must be an integer from 0 through 15 when small packet size is selected and must be an integer from 0 through 31 when large packet size is selected.
- **max-hdr** *value*: Specifies the maximum header size to use. Default: 168. *value* must be an Integer from 0 through 65535.
- **mrru** *value*: Specifies the maximum reconstructed reception unit to use. Default: 65535. *value* must be an Integer from 0 through 65535.

marked-flows-only: Specifies that ROHC is to be applied only to marked flows.
max-hdr *value*: Specifies the maximum header size to use. Default: 168. *value* must be an Integer from 0 through 65535.
mrru *value*: Specifies the maximum reconstructed reception unit to use. Default: 65535. *value* must be an Integer from 0 through 65535.
downlink: Apply the ROHC algorithm only in the downlink direction.
uplink: Apply the ROHC algorithm only in the uplink direction.

Important: When ROHC is enabled for downlink or uplink only the operational mode is Unidirectional.

vj

Specifies that the VJ algorithm is used for header compression.

+

Either one or both of the keywords may be entered in a single command.
If both **vj** and **rohc** are specified, **vj** must be specified first.

Important: If both VJ and ROHC header compression are specified, the optimum header compression algorithm for the type of data being transferred is used for data in the downlink direction.

Usage

Header compression can be used to provide a higher level of security in IP traffic enhance bandwidth usage and lower bit errors.
By default the header compression algorithm is set to **vj**.

Example

The following command disables all IP packet header compression:

```
no ip header-compression
```

The following command sets IP header compression to default vj algorithm:

```
default ip header-compression
```

The following command also sets the IP header compression to the vj algorithm:

```
ip header-compression vj
```

The following command enables the Internet Protocol Control Protocol (IPCP) to determine which protocol is the optimum algorithm for data in the downlink direction and use either VJ or ROHC as needed:

```
ip header-compression vj rohc
```

The following command enables ROHC for the downlink direction only:

```
ip header-compression rohc downlink
```

The following command enables ROHC in any direction using Bidirectional Optimistic mode:

```
ip header-compression rohc any mode Optimistic
```

ip hide-service-address

Hide the IP address of the service from the subscriber.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ip hide-service-address
```

no

Does not hide the IP address of the service from the subscriber. This is the default behavior.

ip hide-service-address

Hides the IP address of the service from the subscriber.

Usage

Use this command to prevent subscribers from using traceroute to discover the network addresses that are in the public domain and configured on services. This prevent users from pinging such addresses.

ip local-address

Configures the local-side IP address of the subscriber's point-to-point connection.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip local-address *ip_address*

no ip local-address

no

Removes a previously configured IP local-address.

ip_address *ip_address*

Specifies an IP address configured in a destination context on the system through which a packet data network can be accessed. *ip_address* is entered using IPv4 dotted-decimal notation.

Usage

This parameter specifies the IPv4 address on the system that the MS uses as the remote-end of the PPP connection. If no local address is configured, the system uses an "unnumbered" scheme for local-side addresses.

Example

The following command configures a local address of 192.168.1.23 for the MS:

```
local-address 192.168.1.23
```

ip multicast discard

Configures the IP multicast discard packet behavior.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ip multicast discard
```

no

Does not discard IP multicast packets.

ip multicast discard

Discards IP multicast packets.

Usage

This command specifies if IP multicast packets will be discarded.

ip qos-dscp

Configures quality of service (QoS) options for the current subscriber using the differentiated services code point (DSCP) method. This functionality is disabled by default.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip qos-dscp *option*

no ip qos-dscp

no

Sets the quality of service option to its default value.

ip qos-dscp *option*

Default: be (Best Effort)
Specifies the subscriber's per hop quality of service setting as one of:

- **af11**: assured Forwarding 11
- **af12**: assured Forwarding 12
- **af13**: assured Forwarding 13
- **af21**: assured Forwarding 21
- **af22**: assured Forwarding 22
- **af23**: assured Forwarding 23
- **af31**: assured Forwarding 31
- **af32**: assured Forwarding 32
- **af33**: assured Forwarding 33
- **af41**: assured Forwarding 41
- **af42**: assured Forwarding 42
- **af43**: assured Forwarding 43
- **be**: best effort forwarding
- **ef**: expedited forwarding

Usage

Set the quality of service for a subscriber based upon the service level agreements.

Example

```
ip qos-dscp ef
```

```
no ip qos-dscp
```

ip route

Configures the static route to use to reach the subscriber's network.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] ip route *ip_address ip_mask* **[** *gateway_address* **]**

no

Removes the configured route information from the subscriber data.

ip route *ip_address*

Specifies the target IP address for which the route information applies using IPv4 dotted-decimal notation.

ip_mask

Specifies the networking mask for the route.
1 bits in the *ip_mask* indicate that bit position in the *ip_address* must also have a value of 1.
0 bits in the *ip_mask* indicate that bit position in the *ip_address* does not need to match, such as the bit can be either a 0 or a 1.
For example, if the IP address and mask were specified as 172.168.10.0 and 255.255.255.224, respectively, the network mask will be 172.168.0.0 (obtained by logically ANDing the IP address with the IP mask).

gateway_address

Default: assigned remote IP address will be used as the gateway address.
Specifies the IP address of the next hop gateway for the route using IPv4 dotted-decimal notation.

Usage

The static routes are also known as framed IP routes for subscribers. Static routes are typically applicable for subscribers connecting via other networks or when the mobile device acts as a gateway to a network on the far side of the device.
For example, if the mobile device is assigned IP address 10.2.3.4 and it acts as a gateway for the network 10.2.3.0 (with a network mask of 255.255.255.0) a static route would be configured with the *ip_address* being 10.2.3.0, *ip_mask* being 255.255.255.0, and *gateway_address* being 10.2.3.4.

Example

```
no ip route 10.2.3.4 255.255.255.0
```

ip source-validation

Enables or disables packet source validation for the current subscriber. Source validation requires that the source address of the received packets match the IP address assigned to the subscriber (either statically or dynamically) during the session.

If an incorrect source address is received from the mobile node, the system attempts to renegotiate the PPP session. The parameters for IP source validation can be set by the **ip source-violation** command.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] ip source-validation

no

Disables source validation.

ip source-validation

Enables source validation.

Usage

Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Example

The following command enables IP source validation:

```
ip source-validation
```

The following command disables IP source validation:

```
no ip source-validation
```

ip user-datagram-tos copy

Controls copying of the IP TOS octet value from IPv4/IPv6 datagrams to the IP header in tunnel encapsulation. This is disabled by default.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

```
ip user-datagram-tos copy [ access-link-tunnel | both | data-tunnel ]

no ip user-datagram-tos copy
```

no

Disable copying of the IP TOS octet value to all tunnel encapsulation IP headers.

ip user-datagram-tos copy

Enables copying of the IP TOS octet value to all tunnel encapsulation IP headers.

access-link-tunnel

Copies the IP TOS octet value to the tunnel encapsulation IP header on the access side (RP) tunnel.

both

Uses both the access-link-tunnel and data-tunnel.

data-tunnel

Copies the IP TOS octet value to the tunnel encapsulation IP header on the MIP data tunnel or L3 tunnel (IP-in-IP, GRE).

Usage

Use this command to enable the copying of the IP TOS octet value to the tunnel encapsulation IP header. This functionality allows PCF to detect special TOS marking in the outer IP header of A11 packets and to identify certain packets as QChat control messages. The Base Station Controller/Packet Control Function (BSC/PCF) must give higher priority to QChat control messages.

Example

The following command enables copying of the IP TOS octet value to the tunnel encapsulation IP header for the access side tunnel:

```
ip user-datagram-tos copy access-link-tunnel
```

The following command disables copying of the IP TOS octet value to all tunnel encapsulation IP headers:

```
no ip user-datagram-tos copy
```

ip vlan

Configures subscriber-to-Virtual LAN (VLAN) associations.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

ip vlan *vlan-id*

[default | no] ip vlan

default

Resets the VLAN ID to the default setting.

no

Disables the VLAN ID for the subscriber.

ip vlan *vlan-id*

Specifies the VLAN ID that is associated with the IP address for that session. *vlan-id* is an integer from 1 through 4094.

Usage

This command configures the subscriber vlan ID which is used with the assigned address for the subscriber session to receive packets. If the IP pool from which the address is assigned is configured with a VLAN ID, this subscriber configured VLAN ID overrides it.
Subscriber traffic can be routed to specific VLANs based on the configuration of their user profile. Using this functionality provides a mechanism for routing all traffic from a subscriber over the specified VLAN. All packets destined for the subscriber must also be sent using only IP addresses valid on the VLAN or they will be dropped.

Example

Set the vlan ID to the default setting by entering the following command:

```
default ip vlan
```

ipv6 access-group

Configures the IPv6 access group for a subscriber.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

ipv6 access-group *name* **[in | out]**

ipv6 access-group *name*

Defines the access group name. *name* is an alphanumeric string of 1 through 47 characters.

in

Defines the access group as inbound.

out

Defines the access group as outbound.

Usage

Used to create an access group for a subscriber.

Example

The following command provides an example of an IPv6 access group with the name *list_1*:

```
ipv6 access-group list_1
```

ipv6 address

Configures a static IP address for use by the subscriber.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

[no] ipv6 address { prefix *address* **| prefix-pool** *name* **}**

no

Deletes a previously configured ipv6 address.

ipv6 address *address*

Specifies an IPv6 address. *address* is entered using IPv6 colon-separated notation.

prefix

Specifies a static IPv6 address.

prefix-pool *name*

Specifies an IPv6 prefix pool name. *name* is an alphanumeric string of 1 through 31 characters.

Usage

Use this command to assign a static IPv6 address to the subscriber. This address will be used each time the subscriber establishes data sessions.

Example

The following command configures a static IP address of *2001:4A2B::1f3F* with a mask length of *24* to the subscriber:

```
ipv6 address 2001:4A2B::1f3F/24
```

ipv6 dns

Configures the IPv6 Domain Name Service (DNS) servers.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

[no] ipv6 dns { primary | secondary } { *ipv6_dns_address* **}**

no

Deletes a previously configured DNS server.

ipv6 dns *ipv6_dns_address*

Specifies an IP address for the DNS server. *ipv6_dns_address* is entered using IPv6 colon-separated notation.

primary

Configures the primary DNS server for the subscriber.

secondary

Configures the secondary DNS server for the subscriber. Only one secondary DNS server can be configured.

ipv6_dns_address

Configures the IP address of the DNS server.

Usage

DNS servers are configured on a per subscriber basis. This allows each subscriber to use specific servers.

Example

The following command provides an example of setting the primary IPv6 DNS server:

```
ipv6 dns primary fe80::c0a8:a04
```

ipv6 dns-proxy

Configures the system to act as a domain name server proxy for the current subscriber.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] ipv6 dns-proxy
```

default

Disables IPv6 DNS proxy functionality for a subscriber.

no

Removes the pre-enabled functionality of IPv6 DNS proxy for a subscriber.

ipv6 dns-proxy

Enables IPv6 DNS proxy functionality for a subscriber. If enabled, the system will act as a proxy DNS server. Default: disabled.

Usage

Used to enable or disable IPv6 DNS proxy for the subscriber. When enabled, the PDSN acts as a proxy DNS server for DNS IPv6 queries coming from the mobile station to the PDSN's local PPP link address.

Example

The following command disables the IPv6 DNS proxy function for the subscriber:

```
no ipv6 dns-proxy
```

ipv6 egress-address-filtering

Configures the system to perform egress address filtering for the subscriber.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ipv6 egress-address-filtering
```

no

Disables IPv6 egress address filtering.

ipv6 egress-address-filtering

Enables IPv6 egress address filtering.

Usage

Used to enable the filtering of packets that arrive from the Internet to a particular site.

Example

The following command disables egress address filtering:

```
no ipv6 egress-address-filtering
```

ipv6 initial-router-advt

Creates an IPv6 initial router advertisement interval for the subscriber.

Product

PDSN, GGSN, ASN-GW, HSGW, P-GW

Privilege

Security Administrator, Administrator

Syntax

ipv6 initial-router-advt { interval *value* **| num-advts** *value* **| router-solicit-wait-timeout** *value* **}**

default ipv6 initial-router-advt { interval | num-advts | router-solicit-wait-timeout }

no ipv6 initial-router-advt router-solicit-wait-timeout

default

Resets the command to its default settings.

no ipv6 initial-router-advt router-solicit-wait-timeout

Disables running timer to wait for router solicit and sends the initial router advertisement immediately once session is up.

ipv6 initial-router-advt

Enables an initial router advertisement interval in milliseconds.

interval *value*

Default: 3000
The time interval the initial IPv6 router advertisement is sent to the mobile node in milliseconds.
value is an integer between 100 and 16000 milliseconds.

num-advts value *value*

Default: 3
The number of initial IPv6 router advertisements sent to the mobile node. *value* is an integer between 1 to 16.

router-solicit-wait-timeout *value*

Default: 3000
The time interval to wait for router solicit before sending the initial IPv6 router advertisement.
value is an integer between 1 and 30000 milliseconds.

Usage

This command is used to set the advertisement interval and the number of advertisements. Using a smaller advertisement interval increases the likelihood of router being discovered more quickly when it first becomes available.

If timer is enabled and router solicit is received before timeout, then RA will be sent in response to RS and no further RA will be sent. If timer is enabled and no router solicit is received after timeout, initial RAs will be sent as configured and IPv6 capability indication will be sent in S2a to P-GW to indicate that P-GW should drop any IPv6 traffic for this PDN.

Example

The following command specifies the initial ipv6 router interval to be 2000ms:

```
ipv6 initial-router-advt interval 2000
```

ipv6 interface-id

Provides an IPv6 interface identifier for the subscriber.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

ipv6 interface-id *ifid*

[default | no] ipv6 interface-id

default

No interface ID set for IPv6CP negotiation to subscriber.

no

Deletes a previously configured IPv6 interface ID.

interface-id *ifid*

Specifies the interface ID assigned to the Mobile during IPv6 Control Protocol (IPv6CP) negotiation. *ifid* is a 64-bit unsigned integer.

Usage

Used to provide a IPv6 ifid for the subscriber when using IPv6-to-IPv4 (6to4)routing.

Example

The following command provides an example of assigning an IPv6 interface ID of *00-00-00-05-47-00-37-44* to the subscriber:

```
ipv6 interface-id 00-00-00-05-47-00-37-44
```

ipv6 minimum-link-mtu

Configures the IPv6 minimum link maximum transmission unit (MTU) value.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

ipv6 minimum-link-mtu *value*

default ipv6 minimum-link-mtu

default

Resets minimum link MTU to its default setting: 1280.

ipv6 minimum-link-mtu *value*

Specifies the MTU (in bytes) as a minimum link value. *value* is an integer between 100 and 2000.

Usage

Used to override the IPv6 minimum link MTU values recommended by the standard.

Example

The following command provides an example of assigning an IPv6 minimum link MTU to *1580* to the subscriber:

```
ipv6 minimum-link-mtu 1580
```

ipv6 secondary-address

Configures additional IPv6 4-bit prefixes to the subscriber session.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

[no] ipv6 secondary-address { prefix *ipv6_address_prefix* **| prefix-pool** *pool_name* **}**

no

Deletes a previously configured ipv6 secondary address.

ipv6 secondary-address *ipv6_address_pref*

Specified the secondary IPv6 address using IPv6 colon-separated notation.

pool_name

Specifies the name given to the secondary address prefix pool as an alphanumeric string of of 1 through 31 characters.

Usage

An IPv6 prefix pool name may be configured for a dynamic prefix, while the prefix is static. This command may be executed multiple times to configure multiple prefixes.

Example

The following command assigns an IPv6 secondary address prefix-pool name of *eastcoast* to the subscriber:

```
ipv6 secondary-address prefix-pool eastcoast
```

l2tp send accounting-correlation-info

Enables the sending of accounting correlation information (Correlation-Id, NAS-IP-Address and NAS-ID) by the L 2TP Access Concentrator (LAC) in L2TP control messages (ICRQ) during session setup to an L2TP Network Server (LNS).

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no | default ] l2tp send accounting-correlation-info
```

no

Disables the sending of accounting correlation information by the LAC.

default

Sets the setting to default mode: disable.

l2tp send accounting-correlation-info

Enables the sending of accounting correlation information by the LAC.

Usage

Use this command to enable the LAC to send accounting correlation information (Correlation-Id, NAS-IP-Address and NAS-ID) in L2TP control message (ICRQ) during session setup to LNS for this subscriber. LNS can be configured to include this information in ACS billing records, so that billing servers can easily correlate accounting records from PDSN/LAC and LNS.
By default, this mode is disabled.

Example

The following command disables the inclusion of accounting correlation information in control messages during session setup to an LNS for a subscriber:

```
default l2tp send accounting-correlation-info
```

l3-to-l2-tunnel address-policy

Configure the subscriber address allocation/validation policy, when subscriber Layer 3 (IPv4) sessions are tunneled using Layer 2 tunneling protocol (L2TP).

Product

HA, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
l3-to-l2-tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }

default l3-to-l2-tunnel address-policy
```

default

Restores the default value for Layer 3-to-Layer 2 tunnel addressing: **no-alloc-validate**.

l3-to-l2-tunnel address-policy

Sets the policy for Layer 3-to-Layer 2 sessions to one of the following options.

alloc-only

Only allocates an address in the case of dynamic address assignment. Does not validate static addresses.

alloc-validate

Locally allocates and validates the subscriber addresses.

no-alloc-validate

Does not allocate or validate subscriber addresses locally for current subscribers sessions. Passes the address between the remote tunnel terminator and the Mobile Node. This is the default behavior.

Usage

Use this command to configure the L3 to L2 tunnel address policy for MIP HA sessions tunneled from the system using L2TP tunnels or for GGSN IP Context sessions tunneled using L2TP to a remote LNS. Also refer to the **resource** keyword of the Context Configuration mode **ip pool** command.

Example

the following command sets the L3-to-L2 tunnel address policy so that the current subscriber must have IP addresses allocated and validated locally on the system:

```
l3-to-l2-tunnel address-policy alloc-validate
```

loadbalance-tunnel-peers

Configures the load balancing of traffic bound for L2TP tunnels configured on the system for the selected subscriber.

Product

L2TP

Privilege

Security Administrator, Administrator

Syntax

```
loadbalance-tunnel-peers { balanced | prioritized | random }
```

loadbalance-tunnel-peers

Enables load balancing of L2TP traffic using one of the methods described below.

balanced

Enables the equal use of all configured tunnel peers (LNSs) for the selected subscriber.

prioritized

Enables the use of all configured tunnel peers (LNSs) for the selected subscriber based on the preference number assigned to the peer address.

random

Default: Enabled
Enables the random use of all configured tunnel peers (LNSs) for the selected subscriber.

Usage

Use to manage traffic loads on L2TP Access Concentrator (LAC) ports and their respective L2TP Network Servers (LNSs).

Example

Use the following command to randomly use all configured tunnel peers (LNSs):

```
loadbalance-tunnel peers random
```

long-duration-action

Specifies what action is taken when the long duration timer expires.

Product

All

Privilege

Administrator

Syntax

```
long-duration-action { detection | disconnection [ dormant-only ] [ suppress-notification ] }
```

detection

Default: Enabled
Detects long duration sessions and sends SNMP TRAP and CORBA notification. This is the default behavior. Use this command to detect a session exceeding the limit set by the long duration timer.

disconnection [dormant-only] [suppress-notification]

Default: Disabled
Detects a long duration session and disconnects the session after sending SNMP trap and CORBA notification.
suppress-notifiaction: Suppresses the SNMP trap and CORBA notification after detecting and disconnecting a long duration session. Default: Disabled
dormant only: Disconnects the dormant sessions after long duration timer and inactivity time with idle time-out duration expires. If the long duration timeout is fired and the call is not dormant, the call is disconnected when the call later moves to dormancy.

Important: For HA calls, the inactivity-time is considered as gauge for dormancy.

It sends the SNMP trap and CORBA notification after disconnecting a long duration session. Default: Disabled

Usage

Use this command to determine what action is taken when a session exceeds the limit set by the long duration timer.

Example

Use the following command to enable disconnecting sessions that exceed the long duration timer:

```
long-duration-action disconnection
```

Use the following command to disconnect the session that exceed the long duration timer without sending SNMP trap and CORBA notification:

```
long-duration-action disconnection suppress-notification
```

Use the following command to disconnect the session that is in dormant and exceed the long duration timer and send SNMP trap and CORBA notification:

long-duration-action disconnection dormant-only

Note that in case of HA calls, the inactivity-time is considered as gauge for dormancy.

max-pdn-connections

Specifies the maximum number of connections to packet data networks (PDNs) supported per eHRPD session.

Product

HSGW

Privilege

Security Administrator, Administrator

Syntax

max-pdn-connections *eHRPD_PDNs*

default max-pdn-connections

default

Resets the maximum number of PDN connections supported per eHRPD session to 3.

max-pdn-connections *eHRPD_PDNs*

Specifies the maximum number of PDN conceitedness allowed per eHRPD session. *eHRPD_PDNs* must be an integer from 1 to 14. Default is 3.

Usage

This command is used to specify the maximum number of PDN connections supported per eHRPD session.

Example

The following command specifies a maximum of *5* PDNs per eHRPD session:

```
max-pdn-connections 5
```

mediation-device

Enables the use of a mediation device for subscribers, and specifies the system context to use for communicating with the device. A mediation device can be the initial point of contact for all IT systems that need to receive Charging Data Records (CDRs). Mediation devices can also be deep-packet inspection servers or transaction control servers.

Product

GGSN, P-GW PDG, TTG

Privilege

Security Administrator, Administrator

Syntax

mediation-device context-name *<context-name>* **[no interims]**

[no | default] mediation-device

no

Deletes the mediation-device configuration.

default

Changes the mediation device to no context-name configured and restores the mediation device's default properties.

mediation-device context-name *context-name*

Default: The subscriber's destination context.
Configures the mediation VPN context for the subscriber.
context-name must be an alphanumeric string of 1 through 79 characters that is case sensitive. If not specified, the mediation context is same as the destination context of the subscriber.

no-interims

Disables sending of Interim messages to the mediation device.
Default: Disabled

Usage

This command is used to enable mediation device support for subscribers.
Keywords to this command can be used in combination to each other, depending on configuration requirements.

Example

The following command enables mediation device support for the subscriber and uses the protocol configuration located in an system context called *ggsn1*:

```
mediation-device context-name ggsn1
```

mobile-ip

Enables or disables access to mobile IP services by the subscriber.

Product

HA, FA

Privilege

Security Administrator, Administrator

Syntax

[no] mobile-ip { allow-aaa-address-assignment | dns-address source-priority { aaa | home-agent } | gratuitous-arp aggressive | home-agent *ip_address* **[alternate] | match-aaa-assigned-address | mn-aaa-removal-indication | mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } | mn-ha-shared-key** *key* **| mn-ha-spi** *spi_num* **| reverse-tunnel | security-level { ipsec | none } | send { accounting-correlation-info | dns-address | imsi | terminal-verification } }**

no

Disables the mobile IP option specified.

allow-aaa-address-assignment

Default: Disabled.
Enables the FA to accept a home address assigned by an AAA server. This should only be configured on the FA side.

dns-address source-priority { aaa | home-agent }

Sets the priority behavior on the FA to use either the DNS IP address information from the HA or the AAA server to include in the RRP to the MN.
When the **no** keyword is used in conjunction with the **dns-address** keyword, information received from both the home-agent and the AAA server is sent if available.
DNS IP address information from the HA comes from the DNS Normal Vendor/Organization Specific Extension (NVSE) in the Registry Registrar Protocol (RRP).
DNS IP address information from the AAA server is in the access accept message.
home-agent: If the DNS address is received from the home-agent only that information is sent to the MN. Otherwise the DNS address received from the AAA server is sent.
aaa: If the DNS address is received from the AAA server only that information is sent to MN. Otherwise the DNS address received from the home-agent is sent.

gratuitous-arp aggressive

Default: Disabled.
When enabled, this mode will cause the HA to send out gratuitous ARP (Address Resolution Protocol) messages for all Mobile IP (MIP) registration renewals and handoffs.
To disable this mode, use the **no** form of this command.

Important: This mode will only work for IP addresses that have been assigned from a static IP address pool.

home-agent *ip_address* **[alternate]**

Specifies the IP address of the mobile IP user's home agent. *ip_address* must be entered using IPv4 dotted-decimal or IPv6 colon -separated notation.
alternate - Specifies the secondary, or alternate, Home Agent to use when Proxy Mobile IP HA Failover is enabled.

match-aaa-assigned-address

Default: Disabled.
Enables the FA to validate the home address in the RRQ against the one assigned by AAA server. This should only be configured on the FA side.

mn-aaa-removal-indication

Default: Disabled.
When enabled, the MN-FA challenge and MN-AAA Authentication extensions are removed when relaying a Registration Request (RRQ) to the Home Agent (HA)

mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }

Speechifies the encryption algorithm to use.
Default: **hmac-md5**
hmac-md5: Uses HMAC-MD5 hash algorithm, as defined in RFC-2002bis. This is the default algorithm.
md5: Uses the MD-5 hash algorithm.
rfc2002-md5: Uses the MD-5 hash algorithm variant as defined in RFC-2002.

mn-ha-shared-key *key*

Verifies the MN-HA Authentication for a local subscriber in the current context. *key* is an alphanumeric string or a hexadecimal number beginning with "0x" up to 127 bytes

mn-ha-spi *spi_num*

Specifies the Security Parameter Index (SPI) number. *spi_num* must be an integer from 256 through 4294967295.

reverse-tunnel

Default: enabled.
All the mobile IP user to use reverse IP tunnels. The **no** keyword disables this option.

security-level { ipsec | none }

Default: none
Configures the security level needed for the subscriber's traffic.
ipsec: secures both MIP control and data traffic with IPSec.
none: none of the traffic is secured

Important: This keyword corresponds to the 3GPP2-Security-Level RADIUS attribute. This attribute indicates the type of security that the home network mandates on the visited network.

Important: For this attribute, the integer value "3" enables IPSec for tunnels and registration messages, "4" Disables IPSec

send { accounting-correlation-info | dns-address | imsi | terminal-verification }

accounting-correlation-info: Configures whether the FA sends the correlation info to the NVSE in the RRQ. Default is disabled.
dns-address: Enables the HA to send the DNS address NVSE in the RRP. Default is disabled. This should only be enabled on the HA side.
imsi: Configures sending the IMSI NVSE in the RRQ. Default is sending IMSI in custom-1 format.
terminal-verification: Enables the FA to send the terminal verification NVSE in the RRQ. Default is disabled. This should only be enabled on the FA side.

Important: **send dns-address** is a proprietary feature developed for a specific purpose and requires the MN to be able to renegotiate IPCP for DNS addresses and reregister MIP if necessary. Since this feature needs the MN to support certain PPP/MIP behavior, and not all MNs support that particular behavior, **send dns-address** should be enabled only after careful consideration.

Usage

Use as subscriber service contracts change.

Example

```
mobile-ip home-agent 10.2.3.4

no mobile-ip reverse-tunnel
```

mobile-ip ha

Accommodates two Mobile IP (MIP) Home Agent (HA) options in subscriber mode.

Product

PDSN, HA, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

`[ no ] mobile-ip ha { assignment-table` *`name`* **`| ignore-unknown-ha-addr-error }`**

`no`

Disables the mobile IP HA option specified.

`assignment-table` *`name`*

Specifies the name of an existing MIP HA Assignment table. *`name`* must be an alphanumeric string of 1 through 63 characters.

`ignore-unknown-ha-addr-error`

Default is disabled.
Enables or disables the HA to accept or reject the RRQ from a particular subscriber.

Usage

Use this command to assign a MIP HA Assignment table to the current subscriber.
Use this command to disable or enable the HA to accept or reject the RRQ from a particular subscriber when the HA address in the incoming MIP RRQ is not the same as the HA service address. The feature is off by default which causes the RRQ to be rejected with the error code UNKNOWN_HOME_AGENT.

Example

The following command assigns the MIP HA Assignment table named *`Atable1`* to the current subscriber:

```
mobile-ip ha assignment-table Atable1
```

The following command sets **`ignore-unknown-ha-addr-error`** to its default disabled state:

```
no mobile-ip ha ignore-unknown-ha-addr-error
```

mobile-ip reg-lifetime-override

Overrides the Mobile IP (MIP) registration lifetime from HA with value configured for subscriber.

Product

PDSN, HA, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

mobile-ip reg-lifetime-override [*dur* **| infinite]**

[default | no] mobile-ip reg-lifetime-override

mobile-ip reg-lifetime-override*dur*

Default: 100 seconds.
Overrides the MIP registration lifetime from HA for the specified period of time in seconds. *dur* must be an integer from 1 through 65534.

infinite

Sets the MIP registration lifetime override value to infinite for a particular subscriber.

default

Sets the value of mobile IP registration lifetime override option to 100 seconds.

no

Disables the MIP registration lifetime override option.

Usage

Use this command to configure MIP registration-lifetime per realm/domain. This value overrides the default lifetime configured under HA service.

Example

The following command overrides the MIP registration lifetime value from HA service and defaults the MIP registration lifetime to 100 seconds for the current subscriber:

```
default mobile-ip reg-lifetime-override
```

mobile-ip send accounting-correlation-info

Enables the sending call correlation information Normal Vendor/Organization Specific Extensions (NVSEs) to the HA in the MIP Registry Registrar Protocol (RRP).

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] mobile-ip send accounting-correlation-info
```

default

Disables the support for sending call correlation information NVSEs to the HA in MIP RRQ.
This is the default mode.

no

Removes the configured support for sending call correlation information.

Usage

Use this command to support PDSN-Correlation-ID VSE and send the call correlation information.

Example

The following command enables sending call correlation information NVSEs to the HA in MIP RRQ

```
mobile-ip send accounting-correlation-info
```

mobile-ipv6

Configures Mobile IPv6 related parameters for a subscriber.

Product

PDSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] mobile-ipv6 { home-address ipv6_address | home-agent ipv6_address |
home-link-prefix ipv6_address | tunnel mtu value }
```

default

Disables the support for sending call correlation information NVSEs to the HA in MIP RRQ.
This is the default mode.

no

Removes the configured support for sending call correlation information.

home-address *ipv6_address*

Specifies the home address for the subscriber. *ipv6_address* must be entered using IPv6 colon-separated notation.

home-agent *ipv6_address*

Specifies the IPv6 address of the mobile IP user's home agent. *ipv6_address* must be entered using IPv6 colon-separated notation.

home-link-prefix *ipv6_address*

Specifies the IPv6 address of the mobile IP user's home link. *ipv6_address* must be entered using IPv6 colon-separated notation.

tunnel mtu *value*

Configures the tunnel MTU (in bytes) for the IPv6 tunnel between the HA and the mobile node. *value* must be an integer from 1024 through 2000. The default is 1500.

Usage

This command sets the mobile-ipv6 parameters for a subscriber. Use this command to set the home-address, home-agent, and home-link prefix

Example

Use the following command to set the tunnel MTU value to *1800*:

```
mobile-ipv6 tunnel mtu 1800
```

nai-construction-domain

After authentication, the domain name specified by this command replaces the Network Access Identifier (NAI) constructed for the subscriber.

Product

All

Privilege

Security Administrator, Administrator

Syntax

nai-construction-domain *domain_name*

no nai-construction-domain

nai-construction-domain *domain_name*

Defines the domain name to use to replace the NAI constructed domain name. *domain_name* must be an alphanumeric string of 1 through 79 characters.

no

Deletes the defined domain name.

Usage

Define or delete a domain name to use to replace the NAI constructed domain name after authentication.

Example

the following command sets the domain name to *private1*:

```
nai-construction-domain private1
```

To delete the previously configured domain name, use the following command:

```
no nai-construction-domain
```

nbns

Configures and enables use of NetBIOS Name Service for the subscriber.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
nbns { primary IPv4-address | secondary IPv4-address }

no nbns { primary [ IPv4-address ] | secondary [ IPv4-address ] }
```

nbns primary

Designates primary NBNS server. Must be followed with IPv4 address in dotted-decimal notation.

nbns secondary

Designates secondary/failover NBNS server. Must be followed with IPv4 address in dotted-decimal notation.

IPv4-address

Specifies the IP address used for this service using IPv4 dotted-decimal notation.

no

Removes/disables use of a previously configured NetBios Name Service.

Usage

This command specifies NBNS parameters. The NBNS option is present for both PDP type IP and PDP type PPP for GGSN.
The system can be configured to use of NetBIOS Name Service for the Access Point Name (APN).

Example

The following command configures the subscriber's NetBIOS Name Service to primary IP *192.168.1.15*:

```
nbns primary 192.168.1.15
```

nexthop-forwarding-address

Configures the next hop forwarding address for the subscriber.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

nexthop-forwarding-address *ip_address*

no nexthop-forwarding-address

nexthop-forwarding-address *ip_address*

Configures the IP address of the nexthop forwarding address. *ip_address* must be entered using IPv4 dotted-decimal or IPv6 colon-separated notation.

no

Disables this function. This is the default setting.

Usage

Use this command to configure the next hop forwarding address for the subscriber.

Example

The following command configures the next hop forwarding address to *10.1.1.1* (IPv4):

```
nexthop-forwarding-address 10.1.1.1
```

npu qos

Configures an Network Processing Unit (NPU) QoS priority queue for packets from the subscriber.

Product

PDSN, GGSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

```
npu qos traffic priority { best-effort | bronze | derive-from-packet-dscp | gold | silver
}
```

best-effort

Assigns the best-effort queue priority. This is the lowest priority.

bronze

Assigns the bronze queue priority. This is the third-highest priority.

derive-from-packet-dscp

Default: Enabled
Specifies that the priority is to be determined from the DS field in the packet's TOS octet.

gold

Assigns the gold queue priority. This is the highest priority.

silver

Assigns the silver queue priority. This is the second-highest priority.

Usage

This command is used in conjunction with the Network Processing Unit (NPU) Quality of Service (QoS) functionality.
The system can be configured to determine the priority of a subscriber packet either based on the configuration of the subscriber, or from the differentiated service (DS) field in the packet's TOS octet (representing the differentiated service code point (DSCP) value).
Refer to the *System Administration Guide* for additional information on NPU QoS functionality.

Important: This functionality is not supported for use with the PDSN at this time.

Example

The following command configures the subscriber's priority queue to be gold:

```
npu qos traffic priority gold
```

nw-reachability-server

Binds the name of a configured network reachability server to the current subscriber and enables network reachability detection.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

nw-reachability server *server_name*

no nw-reachability server

nw-reachability server *server_name*

Specifies the name of a network reachability server that has been defined in the current context. *server_name* is an alphanumeric string of 1 through 16 characters.

no nw-reachability server

Deletes the name of the network reachability server from the current subscribers configuration and disable network reachability failure detection for the current subscriber.

Usage

Use this command to define the network reachability server for the current subscriber and enable network reachability failure detection for the current subscriber. If a network reachability server is defined in an IP pool, that setting takes precedence over this command.

Important: Refer to the HA configuration mode command **policy nw-reachability-fail** to configure the action that should be taken when network reachability fails.

Important: Refer to the context configuration mode command **nw-reachability server** to configure network reachability servers.

Important: Refer to the **nw-reachability server server_name** keyword of the **ip pool** command in the *Context Configuration Mode Commands* chapter to bind the network reachability server to an IP pool.

Example

To bind a network reachability server named *InternetDevice* to the current subscriber, enter the following command:

```
nw-reachability server InternetDevice
```

outbound

Configures the subscriber host password for use when authenticating PPP sessions.

Product

All

Privilege

Security Administrator, Administrator

Syntax

outbound [encrypted] password *pwd*

no outbound password

[outbound encrypted] password *pwd*

Specifies the password to use for point-to-point protocol session host authentication. The **encrypted** keyword indicates the password specified uses encryption.
The password specified as *pwd* must be an alphanumeric string of 1 through 63 characters without encryption, or 1 through 127 characters with encryption.
The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

no outbound password

Clears the outbound password configuration from the subscriber data.

Usage

Sets the outbound (egress) password for increased security.

Example

outbound password *secretPwd*

outbound encrypted password *scrambledPwd*

no outbound password

overload-disconnect

Sets the threshold parameter for overload disconnect.

Product

ASN-GW, HA,PDIF, PDSN,PHS GWPDG/TTG

Privilege

Security Administrator, Administrator

Syntax

overload-disconnect [threshold { inactivity-time *inactivity_time_threshold* **| connect-time** *connect_time_threshold* **}]**

[default | no] overload-disconnect [threshold { inactivity-time | threshhold connect-time }]

threshold inactivity-time *inactivity_time_threshold*

Sets the inactivity time threshold (in seconds) as an integer from 0 through 4294967295. The default value of zero disables this feature. If *inactivity-time* for the subscriber's session is greater than *inactivity_time_threshold*, the session becomes a candidate for disconnection.

threshold connect-time *connect_time_threshold*

Sets the connection time threshold (in seconds) as an integer from 0 through 4294967295. A value of zero disables this feature. If connect-time for the subscriber's session is greater than *connect_time_threshold*, the session becomes a candidate for disconnection.

default

Enables the default condition for this subscriber.

no

Disables the overload disconnect feature for this subscriber. This is the default condition for PDIF.

Usage

Set a subscriber's overload disconnect threshold in seconds, based on either inactivity or connection time. When this threshold is exceeded during a session, the subscriber's session becomes a candidate for disconnection. To set overload-disconnect policies for the entire chassis, see **congestion-control overload-disconnect** in the *Global Configuration Mode Commands* chapter.

Example

```
overload-disconnect threshold inactivity-time 120

default overload disconnect threshold connect-time

no overload-disconnect threshold connect-time

no overload disconnect
```

password

Configures the subscribers password for the current context.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ encrypted ] password pwd

no password
```

encrypted

Indicates the password provided is encrypted.
The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

pwd

Specifies the user's password for authentication. *pwd* must be an alphanumeric string of 1 through 63 characters without encryption, or from 1 through 127 characters with encryption. A "null" password is allowed and is entered as consecutive double quotes (" "). See Example(s) for correct syntax.

Important: Subscribers configured with a null password will be authenticated using PAP and CHAP (MD5) only. Subscribers configured without a password (**no password**) will only be able to access services if the service is configured to allow no authentication.

no

Used to clear the subscriber password configuration from the subscriber data.

Important: Subscribers with no password will only be able to access services if the service is configured to grant access with no authentication.

Usage

Password management is critical to system security and all precautions should be taken to ensure passwords are not shared or to easily deciphered.

Example

```
password secretPwd

password ""

no password
```

pdif mobile-ip

Configures PDIF subscriber call setup parameters.

Product

PDIF

Privilege

Security Administrator, Administrator

Syntax

[default | no] pdif mobile-ip { release-tia | required | simple-ip-fallback }

[default | no]

Disables the option specified.

release-tia

Specifies that after subscriber call setup is complete, the tunnel inner address (TIA) is released. If SImple IP is enabled, the TIA becomes the principal communications tunnel and the restriction that it is only to be used to set up a Mobile-IP call is lifted. This parameter is disabled by default.

required

Specifies that Mobile IP is required for this subscriber whenever a call is set up. This parameter is disabled by default.

simple-ip-fallback

Specifies that Simple IP should be used when Mobile IP could not be established. This parameter is disabled by default.

Usage

Use this command to configure specific behavior for the PDIF subscriber during call setup.

Example

The following command enables the system to fall back to Simple IP when Mobile IP fails for this subscriber during call setup:

```
pdif mobile-ip simple-ip-fallback
```

permission

Enables or disables the subscriber's ability to access wireless data services.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] permission { ha-mobile-ip | pdsn-mobile-ip | pdsn-simple-ip }
```

no

Disables the usage of the specified service.

ha-mobile-ip | pdsn-mobile-ip | pdsn-simple-ip

ha-mobile-ip: enables or disables the Home Agent (HA) support for Mobile IP (MIP) service.
pdsn-mobile-ip: enables or disables packet data and Foreign Agent (FA) support for MIP service.
pdsn-simple-ip: enables or disables packet data support for simple IP service.

Usage

Grants the subscriber access to services in the current context.

Example

```
permission pdsn-mobile-ip

no permission ha-mobile-ip
```

policy ipv6 tunnel

Sets maximum transmission unit (MTU) behavior for the IPv6 tunnel between the HA and Mobile Node.

Product

PDSN, HA

Privilege

Security Administrator, Administrator

Syntax

policy ipv6 tunnel mtu exceed { fragment | notify-sender }

mtu exceed { fragment | notify-sender }

fragment: Adjusts tunnel MTU and fragment packets
notify-sender: Sends an ICMPv6 Packet Too Big message to the original sender

Usage

Use this command to configure MTU behavior for an IPv6 tunnel between the HA and Mobile Node.

Example

```
policy ipv6 tunnel mtu exceed fragment
```

policy-group

Assigns or removes a flow-based traffic policy group to a subscriber.

Product

PDSN, HA, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

[no] policy-group *policy_group_name* **direction { in | out }**

no

Removes assigned policy group from a subscriber configuration.

policy-group *policy_group_name*

Specifies the traffic policy group name for a subscriber session flow pre-configured within a destination context. *policy_group_name* is an alphanumeric string of 1 through 15 characters that is case sensitive.

direction { in | out }

Specifies the direction of flow in which the traffic policies need to be applied.

- **in**: specifies the incoming traffic
- **out**: specifies the outgoing traffic

Usage

Use this command to assign a traffic policy group to a subscriber for traffic policing.

Example

```
policy-group traffic_policy_group1 direction in
```

ppp

Configures the point-to-point protocol (PPP) options for the current subscriber.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

ppp { accept-peer-ipv6-ifid | always-on-vse-packet | data-compression { mode { normal | stateless } | protocols { *protocols* [*protocols*] } | ip-header-compression negotiation { detect | force | vj compress-slot-id { both | none | receive | transmit } } | ipv4 { disable | enable | passive } | ipv6 { disable | enable | passive } | keepalive *seconds* | min-compression-size *min_octets* | mtu *max_octets* | remote-renegotiation disconnect { always | nai-prefix-msid-mismatch } }

default ppp { accept-peer-ipv6-ifid | always-on-vse-packet | data-compression { mode | protocols } | ip-header-compression negotiation [vj compress-slot-id] | ipv4 | ipv6 | keepalive | min-compression-size | mtu | remote-renegotiation disconnect }

no ppp { accept-peer-ipv6-ifid | always-on-vse-packet | data-compression protocols | ipv4 | ipv6 | keepalive | mtu | remote-renegotiation disconnect }

---

default

Restores the default value for the option specified.

---

no

Resets the option specified to its default.

---

always-on-vse-packet

Default: Enabled
If this feature is enabled, the PDSN sends special 3GPP2 VSE PPP packets to the Mobile Node with a maximum inactivity timer value. This configuration is applicable only for PDSNsessions.

---

accept-ipv6-peer-ifield

Default: None
Configures an IPv6-to-IPv4 (6to4) tunnel and controls the behavior of IPv6CP negotiation for the Interface ID. If enabled, PDSN will accept a valid interface-id proposed by the peer.

---

data-compression { mode { normal | stateless } | protocols { *protocols* [*protocols*] }

Default: all protocols enabled.
Specifies the subscriber's mode of data compression or the compression protocol to use.
mode: sets the mode of compression where *modes* must be one of:

- **normal**: Packets are compressed using the packet history for automatic adjustment for best compression.

- **stateless**: Each packet is compressed individually.

protocols *protocols*: sets the compression protocol where *protocols* must be one of:

- **deflate**: DEFLATE algorithm
- **mppc**: Microsoft PPP algorithm
- **stac**: STAC algorithm

---

ip-header-compression negotiation { detect | force | vj compress-slot-id { both | none | receive | transmit } }

Default: **force**

detect: The local side does not include the Van Jacobson (VJ) Compression option in its IPCP configuration request unless the peer sends an Internet Protocol Control Protocol (IPCP) NAK including a VJ compression option. If the peer requests the VJ compression option in its IPCP request the local side will ACK/NAK.

force: The IP header compression negotiation in IPCP happens normally. The local side requests the VJ compression option in its IPCP configure request. If the peer side requests VJ compression in its IPCP request, the local side will ACK/NAK the option.

vj compress-slot-id [both | none | receive | transmit]: Configures the direction in which VJ slotid compression should be negotiated.

- **both** - If the client proposes VJ slotid compression, accept it and propose slotid compression for the downlink and uplink.
- **none** - If the client proposes VJ slotid compression, NAK the offer, do not propose slotid compression for the downlink.
- **receive** - (Default) If the client proposes VJ slotid compression in the uplink direction accept the configuration.
- **transmit** - Propose VJ slotid compression for uplink.

---

ipv4 { disable | enable | passive }

Default: enable

Controls IPCP negotiation during PPP negotiation.

disable: The PDSN does not negotiate IPCP with the mobile.

enable: The PDSN negotiates IPCP with the mobile.

passive: The PDSN initiates IPCP only when the mobile sends an IPCP request.

---

ipv6 { disable | enable | passive }

Default: enable

Controls IPv6CP negotiation during PPP negotiation.

disable: The PDSN does not negotiate IPCP with the mobile.

enable: The PDSN negotiates IPCP with the mobile.

passive: The PDSN initiates IPCP only when the mobile sends an IPCP request.

---

keepalive *seconds*

Default: 30

Specifies the frequency of sending the Link Control Protocol keepalive messages. *seconds* must be either 0 or an integer from 5 through 14400. The special value 0 disables the keepalive messages entirely.

---

min-compression-size *min_octets*

Default: 128

Specifies the smallest packet (in octets) to which compression may be applied. *min_octets* must be an integer from 0 through 2000.

mtu *max_octets*

Default: 1500
Specifies the maximum transmission unit (MTU) [in octets] for packets. *max_octets* must be an integer from 100 through 2000.

remote-renegotiation disconnect { always | nai-prefix-msid-mismatch }

Default: Disabled
Terminates the already established PPP sessions if they are renegotiated by the remote side by sending LCP Conf-req/nak/ack. The following termination conditions are available:

- **always**: Automatically disconnects the session.
- **nai-prefix-msid-mismatch**: Disconnects the session only if the MSID of the session does not match NAI-Prefix (prefix before "@" for the NAI). The configuration of the renegotiated (new) NAI is used for the matching process.

Usage

Adjust packet sizes and compression to improve bandwidth utilization. Each network may have unique characteristics such that determining the best packet size and compression options may require system monitoring over an extended period of time.

Example

```
ppp data-compression protocols mode stateless

ppp mtu 500

no ppp data-compression protocols

no ppp keepalive
```

prepaid 3gpp2

Enables 3GPP2 compliant prepaid billing support for a subscriber to be configured by 3GPP2 attributes sent from a RADIUS server. If not enabled, prepaid attributes received from the RADIUS server are ignored.

Product

HA, PDSN

Privilege

Security Administrator, Administrator

Syntax

```
prepaid 3gpp2 { accounting [ no-final-access-request ] | duration-quota final-duration-
algorithm { current-time | last-airlink-activity-time | last-user-layer3-activity-time }
| preference { duration | volume } }

default prepaid 3gpp2 { duration-quota final-duration-algorithm | preference }

no prepaid 3gpp2 accounting
```

`default prepaid 3gpp2 { duration-quota final-duration-algorithm | preference }`

Sets the 3GPP2 Pre-paid settings to the default values.
`duration-quota final-duration-algorithm`: Resets the end of billing duration quota algorithm to the default of current-time.
`preference`: Resets the preference to duration, If both duration and volume attributes are present.

`no prepaid 3gpp2 accounting`

Disables 3GPP2 prepaid accounting. All 3GPP2 Prepaid attributes received from a RADIUS server are ignored.

`accounting [ no-final-access-request ]`

Default: Disabled
Enables 3GPP2 prepaid accounting behavior.
Sets the low-watermark for remaining byte credits. *`percentage`* is a percentage of the subscriber sessions total credits. When the low-watermark is reached a new RADIUS access-request is sent to the RADIUS server to retrieve more credits. *`percentage`* must be an integer from 1 through 99.
`no-final-access-request`: Stops sending final online access-request on termination of 3GPP2 prepaid sessions. By default, this option is disabled.

`duration-quota final-duration-algorithm { current-time | last-airlink-activity-time | last-user-layer3-activity-time }`

Defines what behavior marks the end of the billing duration for duration-based quota usage accounting. The default behavior sets the duration quota algorithm to current-time.
Default: current-time
`current-time`: Selects the duration quota as the difference between the session termination timestamp and the session setup timestamp.
`last-airlink-activity-time`: Selects the duration quota as the difference between the last-user-activity timestamp (G17) and the session setup timestamp.

last-user-layer3-activity-time: Selects the duration quota as the difference between the timestamp of the last layer-3 packet sent to or received from the user and the session setup timestamp.

preference { duration | volume }

If both duration and volume RADIUS attributes are present this keyword specifies which attribute has precedence.
Default: duration
duration: The duration attribute takes precedence.
volume: The volume attribute takes precedence

Usage

Use this command to enable prepaid support for a default user or for the default user of a domain alias.

Example

The following command enables 3GPP2 prepaid support for the default user:

```
prepaid 3gpp2 accounting
```

prepaid custom

Enables custom prepaid billing support for a subscriber to be configured by attributes sent from a RADIUS server. If not enabled, prepaid attributes received from the RADIUS server are ignored. The keywords set prepaid values that are used if the corresponding RADIUS attribute is not present. If the RADIUS attribute is present, it takes precedence over these values.

Product

HA, PDSN

Privilege

Security Administrator, Administrator

Syntax

```
prepaid custom { accounting | byte-count compressed | low-watermark percent percentage |
renewal interval seconds } | preference { duration | volume }

default prepaid custom { byte-count | low-watermark }

no prepaid custom { accounting | byte-count compressed | low-watermark | renewal }
```

default prepaid custom { byte-count | low-watermark }

Resets custom prepaid settings to the default values.
byte-count: Resets to the default of basing the prepaid byte credits on the flow of uncompressed traffic.
low-watermark: Disables sending an access request to retrieve more credits when a low watermark is reached.

no prepaid custom { accounting | byte-count compressed | low-watermark | renewal}

byte-count compressed: The prepaid byte credits are based on the flow of uncompressed traffic. This is the default.
low-watermark: Disables the low watermark feature. An access-request is not sent to the RADIUS server until the credits granted for the subscriber session are depleted.
renewal: Disables time-based renewals for prepaid accounting.

accounting

Default: Disabled
Enables custom prepaid accounting behavior.

byte-count compressed

Default: uncompressed.
When compression is used, the prepaid byte credits are based on the flow of compressed traffic. The default is to base the prepaid byte credits on the flow of uncompressed traffic.

low-watermark percent *percentage*

Default: Disabled.
Sets the low-watermark for remaining byte credits. *percentage* is a percentage of the subscriber sessions total credits. When the low-watermark is reached a new RADIUS access-request is sent to the RADIUS server to retrieve more credits. *percentage* must be an integer from 1 through 99.

renewal interval *seconds*

Default:
The time in seconds to wait before sending a new RADIUS access-request to the RADIUS server to retrieve more credits. *seconds* must be an integer from 60 through 65535.

preference { duration | volume }

If both duration and volume RADIUS attributes are present this keyword specifies which attribute has precedence.
Default: duration
duration: The duration attribute takes precedence.
volume: The volume attribute takes precedence

Usage

Use this command to enable prepaid support for a default user or for the default user of a domain alias.

Example

The following command enables custom prepaid support for the default user:

```
prepaid custom accounting
```

prepaid unclassify

This command provides customer specific functionality.

prepaid voice-push

This command provides customer specific functionality.

prepaid wimax

Enables WiMAX prepaid accounting for this subscriber. This feature is disabled by default.

Product

ASN-GW

Privilege

Administrator

Syntax

```
[ no ] prepaid wimax accounting
```

no

Disables WiMAX prepaid accounting for this subscriber.

Usage

Use this command to enable WiMAX prepaid accounting for this subscriber.

proxy-dns intercept list-name

Identifies a proxy DNS intercept rules list for the selected subscriber.

Product

HA

Privilege

Security Administrator, Administrator

Syntax

[no] proxy-dns intercept list-name *name*

no

Removes the intercept list from the subscribers profile.

proxy-dns intercept list-name *name*

Specifies a name of a proxy DNS intercept list used for the selected subscriber.
name is the name of the intercept list expressed as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to identify a proxy DNS rules list for the selected subscriber. For a more detailed explanation of the HA Proxy DNS Intercept feature, see the **proxy-dns intercept-list** command in the *Context Configuration Mode Commands* chapter.

proxy-mip

Configures support for Proxy Mobile IP for the subscriber.

Product

PDSN, GGSN, ASN-GW, PDIF

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] proxy-mip required
```

no

Disables support for Proxy Mobile IP.

required

Enables support for Proxy Mobile IP.

Usage

When enabled through the session license and feature use key, the system supports Proxy Mobile IP to provide a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP. For subscriber sessions using Proxy Mobile IP, R-P and PPP sessions are established as they would for a Simple IP session. However, the AGW/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN while the MN performs only Simple IP processes.

Example

The following command enables proxy mobile IP for the current subscriber:

```
proxy-mip required
```

qos rate-limit

Configure the action on subscriber traffic flow that violates or exceeds the peak/committed data rate under traffic policing functionality. When configured, the PDG/TTG performs traffic policing for the subscriber session. If the GGSN changes the QoS via an Update PDP Context Request, the PDG/TTG uses the new QoS values for traffic policing.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Syntax

```
qos rate-limit { downlink | uplink } [ qci qci_val ] [ burst-size { bytes | auto-readjust
[ duration dur ] } ] [ exceed-action { drop | lower-ip-precedence | transmit } [ violate-
action { drop | lower-ip-precedence | shape [ transmit-when-buffer-full ] | transmit } ]
] | [ violate-action { drop | lower-ip-precedence | shape [ transmit-when-buffer-full ] |
transmit } [ exceed-action { drop | lower-ip-precedence | transmit } ] ] +no qos rate-
limit direction { downlink | uplink } [ qci qci_val ]
```

no

Disables the QoS data rate limit configuration for the subscriber.

---

downlink

Applies the specified limits and actions to the downlink (to the data coming from the GGSN over the Gn' interface).

---

uplink

Applies the specified limits and actions to the uplink (to the data coming from the UE over the IPSec tunnel).

Important: If this keyword is omitted, the same values are used for all classes.

---

qci *qci_val*

qci_val is the QoS Class identifier (QCI) for which the negotiate limit is being set expressed as an integer from 1 through 9. If no qci-val is configured, it will be taken as undefined-qci (same as undefined-qos class).

---

burst-size { *bytes* | auto-readjust [duration *dur*] }

Default: See the *Usage* section for this command
The burst size allowed (in bytes) for peak data rate and committed data rate.
bytes must be an integer from 1 through 6000000.

Important: The minimum value of this parameter should be configured to the greater of the following two values: 1) three times greater than the packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate. If the committed-data-rate parameter is specified, the burst-size is applied to both the committed and peak rates.

auto-readjust [duration *dur* **]** provides the option to calculate the Burst size dynamically while configuring rate-limit. When enabled. the system calculates the burst size using the GGSN QoS-negotiated rate that will be enforced.
Every time there is a change in the rates (due to an updated QoS), the burst sizes will be updated accordingly. This keyword also provides two different burst sizes. One burst size for peak rate and another for committed rate.
By default this keyword is disabled.
duration *dur* specifies the duration of burst in seconds. If the duration is not specified, the default is 1 second. *dur* must be an integer from 1 through 30.

---

exceed-action { drop | lower-ip-precedence | transmit }

Default: See the *Usage* section for this command
Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

- **drop**: Drops the packets.
- **lower-ip-precedence**: Transmits the packets after lowering the ip-precedence.
- **transmit**: Transmits the packets.

---

violate-action { drop | lower-ip-precedence | transmit }

Default: See the *Usage* section for this command
Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **drop**: Drops the packets.
- **lower-ip-precedence**: Transmits the packets after lowering the IP precedence.
- **transmit**: Transmits the packet after lowering the IP precedence.

shape [transmit-when-buffer-full]: Enables traffic shaping and buffers user packets when subscriber traffic violates the allowed peak/committed data rate. The **[transmit-when-buffer-full]** keyword allows the packets to be transmitted when buffer memory is full.
transmit: Transmits the packet

Usage

This command configures APN quality of service (QoS) data rate shaping through traffic policing. This command specifies the actions to take on subscriber flows exceeding or violating allowed peak or committed data rates. The shaping function also provides an enhanced function to buffer the excessive user packets and send them to the subscriber when subscriber traffic drops below the committed or peak data rate limit.

Important: The buffering of user packets in traffic shaping does not apply for real-time traffic.

Important: If the exceed/violate action is set to “lower-ip-precedence”, this command may override the configuration of the **ip qos-dscp** command in the GGSN service Configuration mode for packets from the GGSN to the PDG/TTG. In addition, the GGSN service **ip qos-dscp** command configuration can override the APN setting for packets from the GGSN to the Internet. Therefore, it is recommended that this command not be used in conjunction with this action.

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the PDG/TTG; it accepts all of the PDG/TTG-provided values for the PDP context.

Important: This command should be used in conjunction with the max-contexts command to limit the maximum possible bandwidth consumption by the APN.

For additional information on QoS traffic shaping and policing, see the *System Administration Guide.*

Default Values

The following table displays the default values for each of the traffic classes:

Class: Conversational	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): 16000000 Exceed Action: lower-ip-precedence Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): 8640000 Exceed Action: lower-ip-precedence Violate Action: drop
Class: Streaming	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): 16000000 Exceed Action: lower-ip-precedence Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): 8640000 Exceed Action: lower-ip-precedence Violate Action: drop
Class: Interactive, Traffic Handling Priority: 1	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop
Class: Interactive, Traffic Handling Priority: 2	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop
Class: Interactive, Traffic Handling Priority: 3	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop
Class: Background	
Downlink Traffic: Disabled Peak Data Rate (in bps): 16000000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop	Uplink Traffic: Disabled Peak Data Rate (in bps): 8640000 Committed Data Rate (in bps): n/a Exceed Action: n/a Violate Action: drop

Usage

This command configures the APN quality of service (QoS) data rate shaping through traffic policing/shaping. This command specifies the actions to take on subscriber flows exceeding or violating allowed peak/committed data rates. The shaping function also provides an enhanced function to buffer the excessive user packets and send them to the subscriber when subscriber traffic drops below the committed or peak data rate limit.

Important: The buffering of user packets in traffic shaping does not apply for real-time traffic.

Important: If the exceed/violate action is set to "lower-ip-precedence", this command may override the configuration of the **ip qos-dscp** command in the GGSN service configuration mode for packets from the GGSN to the SGSN. In addition, the GGSN service **ip qos-dscp** command configuration can override the APN setting for packets from the GGSN to the Internet. Therefore, it is recommended that command not be used in conjunction with this action.

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the SGSN (i.e. it accepts all of the SGSN-provided values for the PDP context.

Important: This command should be used in conjunction with the **max-contexts** command to limit the maximum possible bandwidth consumption by the APN.

Default Values:

To calculate the burst size dynamically a new optional keyword **auto-readjust** [**duration** *dur*] is provided with **burst-size** keyword. By default the burst size is fixed if defined in bytes with this command. In other words irrespective of the rate being enforced, burst-size fixed as given in the **burst-size** *bytes* parameter.

For the need of variable burst size depending on the rate being enforced this new keyword **auto-readjust** [**duration** *dur*] is provided. Use of this keyword enables the calculation of burst size as per token bucket algorithm calculation as T=B/R, where T is the time interval, B is the burst size and R is the Rate being enforced.

It also provides different burst size for Peak and Committed data rate-limiting.

If **auto-readjust** keyword is not used a fixed burst size must be defined which will be applicable for peak data rate and committed data rate irrespective of rate being enforced.

If **auto-readjust** keyword is provided without specifying the duration a default duration of 1 second will be taken for burst size calculation.

Example

The following command lowers the IP precedence when the committed-data-rate and the peak-data-rate are violated in uplink direction:

```
qos rate-limit direction uplink violate-action lower-ip-precedence
```

The following command buffers the excess user packets when the subscriber traffic violates the configured peak or committed data-rate bps in uplink direction. Once the peak/committed data rate for that subscriber goes below the configured limit it transmit them. It also transmits them if buffer memory is full:

```
qos rate-limit direction uplink violate-action shape transmit-when-
buffer-full
```

qos traffic-police

Enables and configures traffic policing through bandwidth limitations and action for the subscriber traffic if it exceeds or violates the peak or committed data rate. Uplink and downlink limits are configured separately.

Product

PDSN, HA, GGSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

qos traffic-police direction { downlink | uplink } [burst-size *bytes* **] [committed-data-rate** *bps* **] [exceed-action { drop | lower-ip-precedence | transmit }] [peak-data-rate** *bps* **] [violate-action { drop | lower-ip-precedence | transmit }]**

no qos traffic-police direction { downlink | uplink }

downlink

Applies the specified limits and actions to the downlink (data to the subscriber).

uplink

Apply the specified limits and actions to the uplink (data from the subscriber).

burst-size *bytes*

Default: 3000
Specifies the allowed peak burst size allowed in bytes.
bytes must be an integer from 0 through 4294967295.

Important: This parameter should be configured to at least the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

committed-data-rate *bps*

Default: 144000
Specifies the committed data rate (guaranteed-data-rate) in bits per second (bps).
bps must be an integer from 0 through 4294967295).

exceed-action { drop | lower-ip-precedence | transmit }

Default: lower-ip-precedence
Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:
drop: Drops the packet
lower-ip-precedence: Transmits the packet after lowering the ip-precedence
transmit: Transmits the packet

peak-data-rate *bps*

Default: 256000
Specifies the peak data-rate for the subscriber in bits per second (bps).
bps must be an integer from 0 through 4294967295).

violate-action { drop | lower-ip-precedence | transmit }

Default: drop
Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:
drop: Drops the packet
lower-ip-precedence: Transmits the packet after lowering the IP precedence
transmit: Transmits the packet

no

Disables traffic policing in the specified direction for the current subscriber.

Usage

Use this command to limit the bandwidth a subscriber uses in the uplink and downlink directions.

Important: If the exceed/violate action is set to "lower-ip-precedence", the TOS value for the outer packet becomes "best effort" for packets that exceed/violate the traffic limits regardless of what the **ip user-datagram-tos copy** command is configured to. In addition, the "lower-ip-precedence" option may also override the configuration of the **ip qos-dscp** command. Therefore, it is recommended that command not be used when specifying this option.

Details on the QoS traffic policing can be found in the *System Administration Guide*.

Example

The following command sets an uplink peak data rate of *128000* bps and lowers the IP precedence when the committed-data-rate and the peak-data-rate are exceeded:

```
qos traffic-police direction uplink peak-data-rate 128000 violate-action
lower-ip-precedence
```

The following command sets a downlink peak data rate of *256000* bps and drops packets when the committed-data-rate and the peak-data-rate are exceeded:

```
qos traffic-police direction downlink peak-data-rate 256000 violate-
action drop
```

qos traffic-shape

Enables and configures traffic shaping functionality when buffering the data packets during congestion or when the subscriber exceeds the configured peak or committed data rate limit. The system buffers the data packets during an instantaneous burst and deliver them to the subscriber when traffic flow drops below the peak or committed data rate. Uplink and downlink traffic shaping are configured separately.

Important: This feature is NOT supported for real-time traffic.

Product

PDSN, HA, GGSN, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

```
qos traffic-shape direction { downlink | uplink } [ burst-size bytes ] [ committed-data-rate bps ] [ exceed-action { drop | lower-ip-precedence | transmit } ] [ peak-data-rate bps ] [ violate-action { drop | lower-ip-precedence | buffer [ transmit-when-buffer-full ] | transmit } ] +

no qos traffic-shape direction { downlink | uplink }
```

downlink

Applies the specified limits and actions to the downlink (data to the subscriber).

uplink

Applies the specified limits and actions to the uplink (data from the subscriber).

burst-size *bytes*

Default: 3000
Specifies the allowed peak burst size in bytes.
bytes must be an integer from 0 through 4294967295.

Important: It is recommended that this parameter be configured to at least the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.

committed-data-rate *bps*

Default: 144000
Specifies the committed data rate (guaranteed-data-rate) in bits per second (bps).
bps must be an integer from 0 through 4294967295).

exceed-action { drop | lower-ip-precedence | transmit }

Default: lower-ip-precedence

Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:
drop: Drops the packet
lower-ip-precedence: Transmits the packet after lowering the ip-precedence
transmit: Transmits the packet

---

peak-data-rate *bps*

Default: 256000
Specifies the peak data-rate for the subscriber in bits per second (bps).
bps must be an integer from 0 through 4294967295).

---

violate-action { drop | lower-ip-precedence | buffer [transmit-when-buffer-full] | transmit }

Default: See the *Usage* section for this command
The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:
drop: Drops the packet
lower-ip-precedence: Transmits the packet after lowering the IP precedence
buffer [transmit-when-buffer-full]: Enables traffic shaping and buffers user packets when subscriber traffic violates the allowed peak/committed data rate. The **[transmit-when-buffer-full]** keyword allows the packet to be transmitted when buffer memory is full.
transmit: Transmits the packet

+

More than one of the above keywords can be entered within a single command.

---

no

Disables traffic policing for the specified direction for the current subscriber.

Usage

Use this command to provide the traffic shaping function to a subscriber in the uplink and downlink directions. This feature is providing a traffic flow control different to QoS traffic policing. When a subscriber violates or exceeds the peak data rate instead of dropping the packets, as in QoS traffic policing, this feature buffers subscriber data packets and sends the buffered data when the traffic flow is low or not in congestion state.

Important: If the exceed or violate action is set to "lower-ip-precedence", the TOS value for the outer packet becomes "best effort" for packets that exceed or violate the traffic limits regardless how the **ip user-datagram-tos copy** command is configured. In addition, the "lower-ip-precedence" option may also override the configuration of the **ip qos-dscp** command. Therefore, this command should not be used when specifying this option.

Details on the QoS traffic policing functionality is located in the System Administration Guide.

Example

The following command sets an uplink peak data rate of *128000* bps and lowers the IP precedence when the committed-data-rate and the peak-data-rate are exceeded:

```
qos traffic-shape direction uplink peak-data-rate 12800 violate-action
lower-ip-precedence
```

The following command buffers the excess user packets when the subscriber traffic violates the configured peak-data-rate *256000* bps in downlink direction. Once the peak/committed data rate for that subscriber goes below the configured limit it transmit them. It also transmits them if buffer memory is full:

```
qos traffic-shape direction downlink peak-data-rate 256000 violate-action
buffer transmit-when-buffer-full
```

radius accounting

Sets the RADIUS accounting parameters for the subscriber or domain. This command takes precedence over the similar Context Configuration command and is disabled by default.

Product

All

Privilege

Administrator

Syntax

radius accounting { interim { interval-timeout *timeout* **| normal | suppress } | ip remote-address list-id** *list_id* **| mode { session-based | access-flow-based { none | auxillary-flows | all-flows | main-a10-only } } | start { normal | suppress } | stop { normal | suppress } }**

no radius accounting { ip remote-address list-id *list_id* **| interim [interval-timeout] }**

interim { interval-timeout *timeout* **| normal | suppress }**

interval-timeout *timeout*: Indicates the time (in seconds) between updates to session counters (log file on RADIUS or AAA event log) during the session. *timeout* must be an integer from 50 to 40000000.

Caution: Interim interval settings received from the RADIUS server take precedence over this setting on the system. While the low limit of this setting on the system is a minimum of 50 seconds, the low limit setting on the RADIUS server can be as little as 1 second. To avoid increasing network traffic unnecessarily and potentially reducing network and system performance, do not set this parameter to a value less than 50 on the RADIUS server.

normal: If RADIUS accounting is enabled, sends this Acct-Status-Type message when required by normal operation
suppress: If RADIUS accounting is enabled, suppresses the sending of this Acct-Status-Type message.

ip remote-address list-id *list_id*

Specifies the identification number of the IP address list to use for the subscriber for remote address-based accounting.
list_id: Specifies the RADIUS accounting remote IP address list identifier for remote-address accounting for the subscriber. *list_id* must be an integer from 1 through 65535.
This command is used as part of the Remote Address-based accounting feature and associates the subscriber with a list of remote addresses. Remote address accounting data is collected each time the subscriber communicates with any of the addresses specified in the list.
Remote address lists are configured using the **list** keyword in the **radius accounting ip remote-address** command in the Context Configuration mode.

mode { session-based | access-flow-based { none | auxillary-flows | all-flows | main-a10-only } }

Default: **session-based**
Specifies if the radius accounting mode is either session-based or access-flow-based.

session-based: configures session-based RADIUS accounting behavior for the subscriber - which means a single radius accounting message generated for the subscriber session not separate accounting messages for individual A10 connections or flows.
access-flow-based: configures access-flow-based RADIUS accounting behavior for the subscriber. This offers flexibility by generating separate accounting messages for flows and A10 sessions.

- **all-flows**: Generates separate RADIUS accounting messages per access flow. Separate accounting messages are not generated for data path connections. (For example, separate messages are not sent for the main A10 or auxiliary connections.).
- **auxillary-flows**: Generates RADIUS accounting records for the main data path connection and for access-flows for all auxiliary data connections. (For example, separate RADIUS accounting messages are generated for the main A10 session and for access-flows within auxiliary A10 connections. The main A10 session accounting does not include octets or other accounting information from the auxiliary flows.)
- **main-a10-only**: Configures access-flow-based single accounting messages (for example only single start/interim/stop) are generated for the main A-10 flows only.
- **none**: Generates separate RADIUS accounting messages for all data path connections (for example, PDSN main or auxiliary A10 connections) but not for individual access-flows. This is essentially A10 connection-based accounting.

---

start { normal | suppress }

normal: If RADIUS accounting is enabled, sends this Acct-Status-Type message when required by normal operation
suppress: If RADIUS accounting is enabled, suppresses the sending of this Acct-Status-Type message.

---

stop { normal | suppress }

normal: If RADIUS accounting is enabled, sends this Acct-Status-Type message when required by normal operation
suppress: If RADIUS accounting is enabled, suppresses the sending of this Acct-Status-Type message.

---

no

ip remote-address list-id *list_id*: Deletes the entry for the specified *list_id*.
interim [interval-timeout]: Disables the interim interval setting.

Usage

Use this command to allow a per-domain setting for the RADIUS accounting.

Example

Set the accounting interim interval to one minute (*60* seconds) for all sessions that use the current subscriber configuration:

```
radius accounting interim interval-timeout 60
```

Do not send RADIUS interim accounting messages:

```
radius accounting interim suppress
```

Sets the accounting message start normal for main A-10 flows only.

```
radius accounting mode main-a10-only start normal
```

radius group

Applies a RADIUS server group at the subscriber level for AAA functionality.

Product

All

Privilege

Security Administrator, Administrator

Syntax

radius group *group_name*

{ default | no } radius group

radius *group_name*

Specifies the name of the server group that is used for authentication and/or accounting for the specific subscriber. *group_name* must be an alphanumeric string of 1 through 63 characters. It must have been preconfigured within the same context of subscriber.

default

Sets or restores the default RADIUS server group specified at the context level or in the default subscriber profile.

no

Disables the applied RADIUS group for specific subscriber.

Usage

This feature provides the RADIUS configurables under radius group node. Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual RADIUS server group for subscriber in that context. Each server group consists of a list of AAA servers. IF no RADIUS group is applied for this subscriber or the default subscriber profile, the default server group available at context level is used for accounting and authentication of the subscriber.

Example

Following command applies a previously configured RADIUS server group named *star1* to a subscriber within the specific context:

```
radius group star1
```

Following command disables the applied RADIUS server group for the specific subscriber.

```
no radius group
```

radius returned-framed-ip-address

Sets the policy whether or not to reject a call when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
radius returned-framed-ip-address 255.255.255.255-policy { accept-call-when-ms-ip-not-supplied | reject-call-when-ms-ip-not-supplied }

default radius returned-framed-ip-address 255.255.255.255-policy
```

accept-call-when-ms-ip-not-supplied

Accepts calls when the RADIUS server does not supply a framed IP address and the MS does not supply an address.

reject-call-when-ms-ip-not-supplied

Rejects calls when the RADIUS server does not supply a framed IP address and the MS does not supply an address.

default

Sets the policy to its default of rejecting calls when the RADIUS server does not supply a framed IP address and the MS does not supply an address.

Usage

Use this command to set the behavior for the current subscriber when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

Example

The following command sets the subscriber profile to reject calls when the RADIUS server does not supply a framed IP address and the MS does not supply an address:

```
radius returned-framed-ip-address 255.255.255.255-policy reject-call-when-ms-ip-not-supplied
```

rohc-profile-name

Identifies the robust header compression (RoHC) profile configuration that will be applied to bearer sessions belonging to this subscriber.

Product

HSGW,PDSN

Privilege

Administrator

Syntax

rohc-profile-name *name*

name

Specifies the name of the RoHC profile that the system will use to apply header compression and decompression parameters to bearer session data for this subscriber. *name* must be an existing RoHC profile expressed as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify a RoHC configuration profile to be applied to bearer sessions belonging to this subscriber. RoHC profiles are configured through the Global Configuration Mode using the **rohc-profile** command.

Example

The following command specifies that the RoHC profile named *rohc-cfg1* is to be applied to all bearer sessions belonging to this subscriber:

```
rohc-profile-name rohc-cfg1
```

secondary ip pool

Specifies a secondary IP pool to be used as backup pool for Network Address Translation (NAT).

Important: This command requires the purchase and installation of a license. Please contact your Cisco sales representative for more information.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

secondary ip pool *pool_name*

no secondary ip pool

no

Removes the previous secondary IP pool configuration.

secondary ip pool *pool_name*

Specifies the secondary IP pool name.
pool_name must be an alphanumeric string of 1 through 31 characters.

Usage

Use this command to configure a secondary IP pool for NAT subscribers, which is not overwritten by the RADIUS supplied list. The secondary pool will be appended to the RADIUS supplied IP pool list or subscriber template provided IP pool list, as applicable, during call setup.

Example

The following command configures a secondary IP pool named *test123*:

```
secondary ip pool test123
```

simultaneous

Enables or disables the simultaneous use of both Mobile and Simple IP services.

Product

PDSN, FA, HA, ASN-GW

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] simultaneous simple-and-mobile-ip
```

no

Disables the simultaneous use.

Usage

Subscribers with mobile devices that concurrently support mobile and simple IP services require this option to be set.

Example

```
no simultaneous simple-and-mobile-ip

simultaneous simple-and-mobile-ip
```

timeout

Configures the subscriber session timeouts.

Product

All

Privilege

Security Administrator, Administrator

Syntax

timeout { absolute | idle } *seconds*

no timeout [absolute | idle]

timeout absolute

Default: 0
Specifies the absolute maximum time a session may exist (in seconds) in any state (active or dormant).

timeout idle

Default: 0
Specifies the maximum duration of the session (in seconds) before the system automatically terminates the session due to inactivity.

seconds

Specifies the maximum amount of time (in seconds) before the specified timeout action is activated. *seconds* must be an integer from 0 through 4294967295. The special value 0 disables the timeout specified.

no

Indicates the timeout specified is to be returned to its default behavior. If a timeout value is not specified, all timeouts are set to their default values.

Usage

Reduce the idle timeout to free session resources faster for use by new requests.

Example

```
timeout absolute 18000

no timeout
```

timeout long-duration

Configures the long duration timeout and optionally the inactivity duration of HA subscriber session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

timeout long-duration *ldt_timeout* **[inactivity-time** *inact_timeout* **]**

[no | default]timeout long-duration

no

Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified then all are set to their default behavior.

long-duration *ldt_timeout*

Default: 0
Designates the maximum duration of the session (in seconds) before the system automatically reports/terminates the session.
ldt_timeout must be a value in the range from 0 through 4294967295. The special value 0 disables the timer.

inactivity-time *inact_timeout*

Specifies the maximum amount of time (in seconds) before the specified session is marked as dormant.
inact_timeout must be a value in the range from 0 through 4294967295. The special value 0 disables the inactivity time specified.

Usage

Use this command to set the long duration timeout period and inactivity timer for subscriber sessions. Reduce the idle timeout to free session resources faster for use by new requests.
Refer to the **long-duration-action detection** and **long-duration-action disconnection** commands for more information.

Example

The following command sets the long duration timeout duration to *300* seconds and inactivity timer for subscriber session to *45* seconds:

```
timeout long-duration 300 inactivity-time 45
```

tpo policy

Specifies the Traffic Performance Optimization (TP)) policy for subscribers.

Product

TPO

Privilege

Security Administrator, Administrator

Syntax

tpo policy *tpo_policy_name*

{ default | no } tpo policy

default

Configures the default setting.
Default: Use the default TPO policy configured in the rulebase.

no

Deletes TPO policy from the subscriber configuration.

tpo policy *tpo_policy_name*

Specifies the name of the TPO policy as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify the TPO policy for the subscriber template.

Example

The following command specifies to use the TPO policy named *tpo_policy_110*:

```
tpo policy tpo_policy_110
```

tunnel address-policy

Specifies the policy for address allocation and validation for all tunneled calls (IP-IP, IP-GRE) except L2TP calls. With this command enabled, GGSN IP address validation could be disabled for specified incoming calls.

For GGSN systems, this command can also be specified in the APN Configuration mode (**tunnel address-policy**) which would mean the system defers to the old **l3-to-l2-tunnel address policy** command for calls coming through L2TP tunnels.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }

default tunnel address-policy
```

alloc-only

Allocates IP addresses locally without validation.

alloc-validate

Default.
The VPN Manager allocates and validates all incoming IP addresses from a static pool of IP addresses.

no-alloc-validate

No IP address assignment or validation is done for calls coming in via L3 tunnels. Incoming static IP addresses are passed. This option allows for the greatest flexibility.

default

Resets the tunnel address-policy to **alloc-validate**.

Usage

This command supports scalable solutions for Corporate APN deployment as many corporations handle their own IP address assignments. In some cases this is done to relieve the customer or the mobile operators from the necessity of reconfiguring the range of IP addresses for the IP pools at the GGSN.

Example

The following command resets the IP address validation policy to validate against a static pool of address:

```
default tunnel address-policy
```

The following command disables IP address validation for calls coming through tunnels:

```
tunnel address-policy no-alloc-validate
```

tunnel ipip

Configures IP-in-IP tunnelling parameters for the current subscriber.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

tunnel ipip peer-address *peer_address* **local-address** *local_addr* **]**

no tunnel ipip

peer-address *peer_address*

Specifies the IP address of the external gateway terminating the IP-in-IP tunnel.

local-address *local_addr*

Specifies the IP address of the interface in the destination context originating the IP-in-IP tunnel.

no

Disables IP-in-IP tunneling for the current subscriber.

Usage

Subscriber IP payloads are encapsulated with IP-in-IP headers and tunneled by the GGSN or PDSN to an external gateway.

Example

The following command configures the system to encapsulate subscriber traffic using IP-in-IP and tunnel it from a local address of *192.168.1.100* to a gateway with an IP address of *192.168.1.225*:

```
tunnel ipip peer-address 192.168.1.225 local-address 192.168.1.100
preference 1
```

tunnel ipsec

Configures sessions for the current subscriber to use an IPSec tunnel based on the IP pool corresponding to the subscriber's assigned IP address.

Product

PDSN, GGSN

Privilege

Security Administrator, Administrator

Syntax

```
tunnel ipsec use-policy-matching-ip-pooler-address

no tunnel ipsec use-policy-matching-ip-pooler-address
```

no

Disables the use of the IPSec policy that matches the IP pool that the assigned IP address relates to.

Usage

Use this command to set the current subscribers sessions to use an IPSec policy that is assigned to the IP pool that the subscribers assigned IP address relates to.

Example

The following command enables the use of the policy that matches the IP pool address:

```
tunnel ipsec use-policy-matching-ip-pooler-address
```

tunnel l2tp

Configures L2TP tunnel parameters for the subscriber.

Product

All products supporting L2TP

Privilege

Security Administrator, Administrator

Syntax

tunnel l2tp [peer-address *ip address* **[[encrypted] [secret** *secret*]] [**preference** *number*] **[tunnel-context** *context* **] [local-address** *ip_address* **] [crypto-map** *map_name* **{ [encrypted] isakmp-secret** *secret* **}]]**

no tunnel l2tp [peer-address *ip_address* **]**

---

peer-address *ip_address*

A peer L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). *ip_address* must be an IP address entered using IPv4 dotted-decimal or IPv6 colon-separated format.

[encrypted] secret *secret*

Specifies the shared key (secret) between the L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). *secret* must be an alphanumeric string of 1 through 63 characters that is case sensitive.
encrypted: Specifies the encrypted shared key between the L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). *secret* must be an alphanumeric string of 1 through 128 characters that is case sensitive.
The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

---

preference *number*

Default: 1
Specifies the order in which a group of tunnels configured for this subscriber will be tried. *number* must be an integer from 1 through 65535.

---

tunnel-context *context*

Specifies the name of the context containing ports through which this subscriber's data traffic is to be communicated between this LAC and the LNS. *context* must be an alphanumeric string of 1 through 79 characters.

---

local-address *ip_address*

Specifies a LAC service bind address which is given as a hint that is used to select a particular LAC service. *ip_address* must be an IP address entered using IPv4 dotted-decimal or IPv6 colon-separated notation.

crypto-map *map_name* **{ [encrypted] isakmp-secret** *secret* **}**

Specifies the name of a crypto map that has been configured in the current context. *map_name* must be an alphanumeric string from 1 to 127 alphanumeric characters.
isakmp-secret *secret*: Specifies the pre-shared key for the Internet Key Exchange (IKE). *secret* must be an alphanumeric string of 1 through 127 characters.
encrypted isakmp-secret *secret*: Specifies the pre-shared key for IKE. Encryption must be used when sending the key. *secret* must be an alphanumeric string of 1 through 127 characters.

no

Disables tunneling for the current subscriber. When peer-address is included, the tunneling for that specific L2TP Network Server (LNS) is disabled but tunneling to other configured LNSs is still enabled.

Usage

Use this command to configure specific L2TP tunneling parameters for the current subscriber.

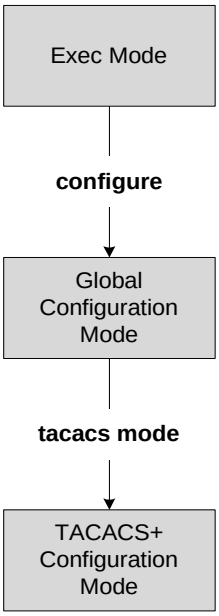
Example

To specify L2tp tunneling to the LNS peer at the IP address *198.162.10.100* with a shared secret of *bigco* and preference of *1*, enter the following command:

```
tunnel l2tp peer-address 198.162.10.100 secret bigco preference 1
```

Chapter 262
TACACS+ Configuration Mode Commands

This chapter describes all commands available in the TACACS+ Configuration Mode. TACACS+ (Terminal Access Controller Access-Control System Plus) is a secure, encrypted protocol. By remotely accessing TACACS+ servers that are provisioned with the administrative user account database, the ASR 000 supports TACACS+ accounting and authentication services for system administrative users.



Important: TACACS Configuration Mode is available in releases 11.0 and later.

accounting

Enables the recording of the start and the stop time each command issued during a TACACS+-authenticated CLI session.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] accounting { start-stop | command }
```

no

Disables a configured TACACS+ accounting setting (either **accounting start-stop** or **accounting command**).

{start-stop | command}

Specifies the type of accounting records to be recorded.

- **start-stop**: Records the time at which the session starts (the time at which the user passes authentication) and the time at which the user exits. If a user exits before passing authentication, only a stop time is recorded.
- **command**: Enables accounting on a command-by-command basis. The TACACS+ server is contacted prior to the execution of the command and the command which is about to be executed is recorded. Only commands which are valid for the user privilege and context (mode) in which they are about to be executed will be recorded. Note that the ASR 5000 does not record whether the command itself succeeded or failed. For security reasons, some secure or restricted commands are not recorded. In such cases, the accounting record will record the command as three asterisks ("***").

Usage

Use this command to configure the accounting method for TACACS+-based CLI sessions.

authorization

Enables the authorization of TACACS+ CLI users on a command-by-command, command + command argument, or command prompt basis. If the user is not authorized to execute the command, the command will fail.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] authorization { command | prompt | arguments }
```

no

Disables a configured TACACS+ authorization **command**, **prompt**, or **arguments** setting.

{ command | prompt | arguments }

Specifies the type of authorization behavior to enforce:

- **command**: Enables per-command authorization. The TACACS+ server is contacted for each command and each command is authorized for the user. If the user is not authorized to execute the command, then the command fails. If the user is authorized for the command, the command is executed.
- **prompt**: Enables per-command authorization, as described for the **command** option above. However, since commands may be duplicated in different CLI modes, this version of the command authorization also passes the command prompt string to the server. The TACACS+ server is contacted for each prompt and command and must have a matching string for the prompt/command combination. Enabling **prompt** authorization supersedes **command** authorization, since the prompt and command must be authorized together.
- **arguments**: Enables per-command and command + argument authorization. The TACACS+ server authorizes each command and its arguments for the user. If the user is not authorized to execute the command and the corresponding arguments, the command fails. If the command does not contain any arguments, then the command only is passed to the authorization server.

Usage

Use this command to configure the authorization method for TACACS+-based CLI sessions.

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

on-authen-fail

Defines system behavior when an administrative login fails due to a TACACS+ authentication failure. This command also can be used to configure system behavior separately for TACACS+ authentication failures for administrative users accessing the system via the ASR 5000 console port.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
on-authen-fail { continue | stop } [ tty console ]
```

`{ continue | stop }`

Specifies the type of authentication behavior to enforce:

- **`continue`**: After a TACACS+ authentication failure, the system will continue with authentication using non-TACACS+ authentication services.
- **`stop`**: After a TACACS+ authentication failure, the system forces the failed TACACS+ user to exit.

`tty console`

Release 12 and later systems only: Used after the **`stop`** or **`continue`** parameters to specify system behavior for users being authenticated via the ASR 5000 console port:

- **`stop tty console`**: Forces the failed TACACS+ user to exit.
- **`continue tty console`**: The system will continue with authentication using non-TACACS+ authentication services.

Usage

Use this command to configure system behavior for users that fail TACACS+ authentication.

on-network-error

Configures ASR 5000 behavior when a TACACS+ login fails due to a network error. This command also can be used to configure system behavior separately for TACACS+ network error login failures for administrative users accessing the system via the ASR 5000 console port.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
on-network-error { continue | stop } [ tty console ]
```

`continue`

The system will continue with authentication using non-TACACS+ authentication services.

`stop`

The system forces the failed TACACS+ user to exit.

`tty console`

Release 12 and later systems only: Can be used after the **`continue`** or **`stop`** options to specify system behavior for TACACS+ CLI users being authenticated via the console port on the chassis:

- **`stop tty console`**: Forces the failed user to exit when authentication fails.
- **`continue tty console`**: The system will continue with authentication using non-TACACS+ authentication services.

Usage

Use this command to configure system behavior for users who fail TACACS+ authentication due to a network error.

on-unknown-user

Configures ASR 5000 behavior when a TACACS+ server cannot authenticate a given user name. This command also can be used to configure system behavior separately for TACACS+ unknown user login failures for administrative users accessing the system via the ASR 5000 console port.

Important: Some TACACS+ server implementations will not send a Reply message indicating that the user name is invalid. Instead, these types of implementations will accept the username, whether valid or not, and then examine the username and password in combination before sending a Reply message indicating a failed TACACS+ login. In these cases, specifying **`on-unknown-user`** will not enforce the desired system behavior. To avoid this scenario, determine the method the configured TACACS+ servers will use to validate user names before deciding whether specifying the **`on-unknown-user`** command will provide the desired result.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
on-unkown-user { continue | stop } [ tty console ]
```

`{ continue | stop }`

Specifies the particular behavior to enforce:

- **`continue`**: The system continues with authentication using non-TACACS+ authentication services.
- **`stop`**: The system forces the failed TACACS+ user to exit.

[

`tty console`

Release 12 and later systems only: Can be used after the **`continue`** or **`stop`** options to specify the behavior of the system for TACACS+ CLI users being authenticated via the console port on the chassis.

- **`stop tty console`**: The system forces the failed user to exit when authentication fails.
- **`continue tty console`**: The system will continue with authentication using non-TACACS+ authentication services.

Usage

Use this command to configure ASR 5000 behavior for users who fail TACACS+ user name authentication.

server

Configures TACACS+ AAA service-related parameters for use in authenticating ASR 5000 administrative users via a TACACS+ server.

Important: Once a TACACS+ server is configured with the **server** command, TACACS+ AAA services for the ASR 5000 must be enabled using the **aaa tacacs+** command in Global Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

[no] server priority *priority_number* **ip-address** *ip_address* **[service { authentication | authorization | accounting }] [port** *port_number* **] [{ encrypted password** *shared_secret* **| password** *text_password* **| key** *text_password* **}] [timeout** *seconds* **] [retries** *num_retries* **] [nas-source-address** *ip_address* **]**

no

Removes a specified **server priority** from the TACACS+ server list.

priority

Specifies the order in which TACACS+ servers are to be tried. A maximum of three TACACS+ AAA servers can be configured. *priority_number* can be an integer from 1 (highest priority) to 3 (lowest priority). If no server with priority 1 is specified, the next highest priority is used. If the specified priority matches that of a TACACS+ server already configured, any previously defined server configuration parameter(s) for that priority are returned to the default setting(s).

ip-address

Specifies the IP address of the TACACS+ server in IPv4 dotted-decimal notation. Only one IP address can be defined for a given **server priority**

[service { authentication | authorization | accounting }]

service: *Release 12 and later systems only*: Specifies one or more of the AAA services that the specified TACACS+ server will provide. Use of the **service** keyword requires that at lease one of the available services be specified. If the **service** keyword is not used, the ASR 5000 will use the TACACS+ server for all AAA service types. The default is to use authentication, authorization and accounting. Available service types are:

- **authentication**: The specified TACACS+ server should be used for authentication. If a TACACS+ authentication server is not available, TACACS+ will not be used for authorization or accounting.
- **authorization**: The specified TACACS+ server should be used for authorization. If TACACS+ authentication is not used, TACACS+ authorization will not be used. If no authorization server is specified and the user is authenticated, the user will remain logged in with minimum privileges (Inspector level).
- **accounting**: The specified TACACS+ server should be used for accounting. If TACACS+ authentication is not used, TACACS+ accounting will not be used. If no accounting server is specified and the user is authenticated, no accounting will be performed for the user.

port

Specifies the TCP port number to use for communication with the TACACS+ server. *port_number* can be an integer from 1 through 65535. If a port is not specified, the ASR 5000 will use port 49.

[{ encrypted password *shared_secret* **| password** *text_password* **| key** *text_password* **}]**

Specify the encrypted or plain-text password:

- **encrypted password** *shared_secret*: Specifies the encrypted value of the shared secret key. The server-side configuration must match the decrypted value for the protocol to work correctly. If **encrypted password** is specified, specifying **password** is invalid. No encryption is used if this value is null (""). The encrypted password can be an alphanumeric string of 1 through 100 characters. If neither an **encrypted password** or **password** is specified, the ASR 5000 will not use encryption
- **password** *plain_text_password*: **Release 12.0 and later systems**. Instead of using an encrypted password value, the user can specify a plain-text value for the password. If the **password** keyword is specified, specifying **encrypted password** is invalid. A null string (“”) represents no encryption. The password can be an alphanumeric string of 1 through 32 characters. If neither an **encrypted password** or **password** is specified, then the ASR 5000 will not use encryption.
- **key** *plain_text_password*: **Release 11.0 systems only**. Instead of using an encrypted password value, the user can specify a plain-text key value for the password. If the **key** keyword is specified, then specifying **encrypted password** is invalid. A null string represents no encryption. The password can be from 1 to 32 alphanumeric characters in length. If neither an **encrypted password** or **key** is specified, then the ASR 5000 will not use encryption.

[timeout *seconds* **]**

Specifies the number of seconds to wait for a connection timeout from the TACACS+ server. *seconds* can be an integer from 1 through 1000. If no timeout is specified, the ASR 5000 will use the default value of 10 seconds.

[

retries *number*

Release 12 and later systems only: Specifies the number of retry attempts at establishing a connection to the TACACS+ server if the initial attempt fails. **retries** *number* can be an integer from 0 through 100. The default is 3. Specifying 0 (zero) retries results in the ASR 5000 trying only once to establish a connection. No further retries will be attempted.

nas-source-address *ip_address*

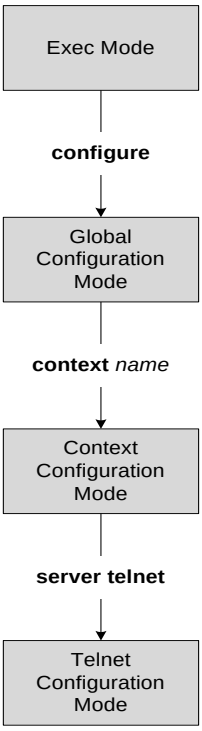
Release 12 and later systems only: Sets the IPv4 address to be specified in the Source Address of the IP header in the TACACS+ protocol packet sent from the NAS to the TACACS+ server. *ip_address* is entered using IPv4 dotted-decimal notation and must be valid for the interface.

Usage

Use this command to specify TACACS+ service parameters for a specified TACACS+ server.

Chapter 263
Telnet Configuration Mode Commands

The Telnet Configuration Mode is used to manage the telnet server options for the current context.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

max servers

Configures the maximum number of telnet servers that can be started within any 60-second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

Product

All

Privilege

Security Administrator, Administrator

Syntax

max servers *count*

count

Default: 40
Specifies the maximum number of servers that can be spawned in any 6- second interval. *count* must be an integer from 1 through 100.

Usage

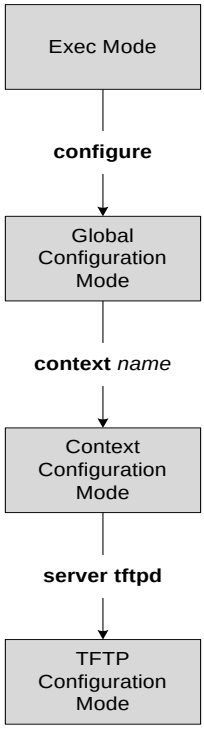
Set the number of servers to tune the system response as a heavily loaded system may need more servers to support the incoming requests.
The converse would be true as well in that a system can benefit by reducing the number of servers such that telnet services do not cause excessive system impact to other services.

Example

```
max servers 50
```

Chapter 264
TFTP Configuration Mode Commands

The TFTP configuration mode is used to manage the TFTP (Trivial File Transfer Protocol) servers for the current context.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

max servers

Configures the maximum number of TFTP servers that can be started within any 60-second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

Product

All

Privilege

Security Administrator, Administrator

Syntax

max servers *count*

count

Default: 40
Specifies the maximum number of servers that can be spawned in any 60-second interval. *count* must be an integer from 1 through 100.

Usage

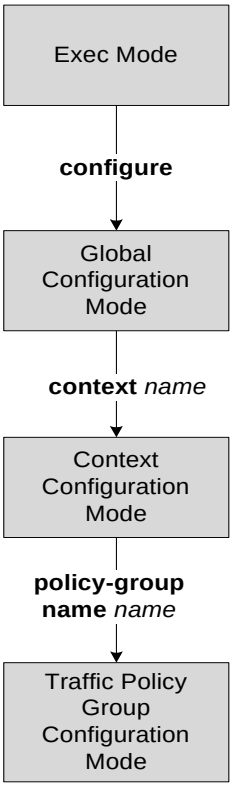
Set the number of servers to tune the system response as a heavily loaded system may need more servers to support the incoming requests.
The converse would be true as well in that a system can benefit by reducing the number of servers such that TFTP services do not cause excessive system impact to other services.

Example

```
max servers 50
```

Chapter 265
Traffic Policy Group Configuration Mode Commands

Policy-Group is used to form a set of configured Policy-Maps for the Traffic Policy feature. Multiple policies can be applied for a subscriber session flow within a destination context.



end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

policy

Assigns traffic policies, pre-configured in Policy-Map Configuration mode, to a Policy Group for flow-based traffic policing of a subscriber session flow.

Product

PDSN, HA, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

[no] policy *policy_map_name* **precedence** *value* **direction [in | out]**

---

no

Disables/removes configured policy for traffic policing.

---

direction [in | out]

Specifies the direction in which the policies need to be applied.

---

policy *policy_map_name*

Specifies the policy name as an alphanumeric string of 1 through 15 characters.

---

precedence *value*

Specifies the precedence of traffic policies to resolve.
value is an integer from 1 through 16. If a session flow matches multiple policies, this keyword resolves them.

Usage

Use this command to form a policy-group with a set of pre-configured Policy-Maps.

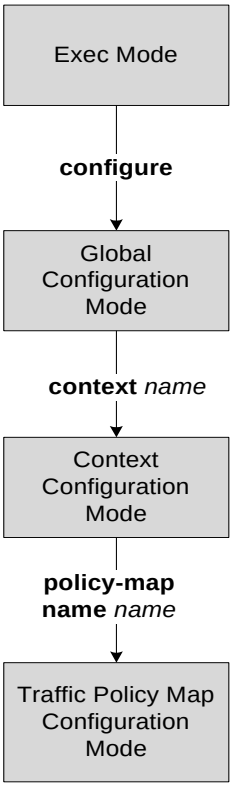
Example

The following commands assigns the traffic policy *policymap1* with precedence *2*.

```
policy policymap1 precedence 2
```

Chapter 266
Traffic Policy-Map Configuration Mode Commands

A Policy-Map imposes a flow-based traffic policy for Traffic Policy feature within a destination context. It designates the flow treatment based on the classification rules configured in Class-Map mode for a subscriber session flow.



3gpp2 data-over-signaling

Configures 3GPP2-related flow treatment policy for the flow-based traffic policing of subscriber sessions.

Product

PDSN, HA, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

3gpp2 data-over-signaling marking [class-map *class_name* **]**

no 3gpp2 data-over-signaling marking

no

Disables configured 3GPP2-related flow treatment policy.

class-map *class_name*

Associates class map to be used for selective data over signaling (DOS) marking. *class_name* is an alphanumeric string of 1 through 15 characters.

marking

Indicates 3GPP2-related traffic flow for data over signaling channel.

Usage

Use this command to mark traffic flows for 3GPP2-related policy.

Example

```
3gpp2 data-over-signaling marking
```

access-control

Configures the access control action for traffic flows matching the Class-Map rules.

Product

PDSN, HA, ASN GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

```
access-control { allow | discard }
```

allow

Allows the packets, if the policy matches with the criteria defined in the Class-Map assigned to the specific traffic policy.

discard

Discards the packets, if the policy matches with the criteria defined in the Class-Map assigned to the specific traffic policy.

Usage

Configures the action or treatment for traffic flows match criteria specified in the assigned Class-Map.

Example

The following command allows the packets or traffic flow on matching with criteria specified in assigned Class-Map for specific traffic policy.

```
access-control allow
```

accounting suppress

Suppresses accounting action for traffic flows matching the policy map.

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] accounting suppress
```

no

Removes the suppression of accounting for traffic flow matching this policy map.

Usage

Use this command to suppress accounting action on traffic flow matching this policy map.
Policy maps configured for accounting suppression are used to implement the QChat Billing Suppression feature that selectively starts and terminates accounting sessions based on the categorization of traffic as being interesting or non-interesting. See the **accounting trigger** command.

Example

The following command configures suppression of accounting on traffic flows matching this policy map:

```
accounting suppress
```

accounting trigger

Configures an accounting trigger policy map to selectively start and terminate accounting sessions based on the categorization of traffic as being interesting or non-interesting. This command supports the QCHAT Billing Suppression feature.

Product

PDSN, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

`[ no | default ] accounting trigger { inactivity-timeout | interesting-traffic | intra-service-handoff }`

`default`

Sets or restores the default value assigned for specified parameter.

`no`

Disables previously configured triggers.

`inactivity-timeout`

Generates an accounting Stop message if there has been no data activity on the session for the interim accounting timeout interval.
Default: disabled

`interesting-traffic`

Generates an accounting Start message upon arrival of interesting traffic.
Default: disabled

`intra-service-handoff`

Generates accounting Start and Stop messages during intra-service handoffs.
Default: enabled
If disabled, the messages are suppressed during the handoffs. The current accounting session continues and no Stop or Start messages are generated during the intra-service handoff.

Usage

Use this command to configure an accounting trigger policy map (ATPM) to selectively start and terminate accounting sessions based on the categorization of traffic as being interesting or non-interesting. This command supports the QChat Billing Suppression feature.
Interesting traffic is identified as traffic that does not match any of the other Accounting Policy Maps (APMs) configured for accounting suppression. See the **`accounting suppress`** command.
An ATPM is similar to an APM, but without the class map rules. The ATPM is configured as of type accounting using the **`type accounting`** command.
Optionally, timeout can be triggered when there is no data traffic for the interim accounting timeout interval using the **`accounting trigger inactivity-timeout stop`** command. On timeout, the accounting

session is terminated and an Accounting Stop message is sent. A new accounting session is created if interesting traffic resumes.
In the ATPM, the trigger to start accounting for interesting traffic is configured using the **accounting trigger interesting-traffic** command. Accounting Start is triggered on arrival of interesting traffic, or change in airlink parameters conveyed through active-start airlink record. If an active-start record was included in the initial connection setup, Accounting Start is not triggered. But if the active-start comes separately and is the first one for the session, it is treated as airlink change and an Accounting Start is sent. The ATPM should have the lowest precedence among the APMs.
As the airlink events are generated on the ingress side, the ATPM must be included in a policy group that is applied to the ingress direction in the subscriber profile. The configuration is applicable only for standard trigger policy and session based accounting mode.

Example

The following command sets the trigger to generate accounting start message upon arrival of interesting traffic:

```
accounting trigger interesting-traffic
```

class-map

Assigns a traffic classification rule (Class-Map) to the policy map.

Product

PDSN, HA, ASN GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

[no] class-map *name*

no

Enables or disables **class-map**.

name

Specifies the name of the class map assigned for this policy map. The class map should have been preconfigured via the Class Map Configuration Mode.
name must be an alphanumeric a string of 1 through 15 characters.

Usage

Use this command to assign a class map to the policy map for traffic policing. The class map is configured in the Class Map Configuration Mode.

Example

The following command assigns the class map *classification1* to the current policy map:

```
class classification1
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

flow-tp-trigger

This command specifies that the traffic volume will be calculated based on the traffic on the flow.

Product

PDSN, HA, ASN GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

flow-tp-trigger volume *traffic_volume_threshold*

no flow-tp-trigger volume

traffic_volume_threshold

Specifies the volume threshold to trigger traffic policing. *volume* must be an integer from 1 through 4294967295.

Usage

This command is available if you have purchased and installed the Intelligent Traffic Control License on your system. Use this command to calculate the traffic volume based on the traffic on the flow.

Example

```
flow-tp-trigger volume 500
```

ip header-compression

Enables the system to mark IP flows for Robust Header Compression (RoHC).

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ip header-compression rohc flow-marking
```

no

Disables the setting.

rohc flow-marking

Marks the IP flow for SO67 and PPP RoHC.

Usage

Use this command to mark IP flows for SO67 and PPP RoHC.

Example

```
ip header-compression rohc flow-marking
```

qos encaps-header

Enables and configures Quality of Service (QoS) policy to use Differentiated Service Code Point (DSCP) marking in IP header fields for the flow-based traffic policing to subscriber session flow.

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

qos encaps-header dscp-marking { *dscp_code* | copy-from-user-datagram [ignore-pcf-signaled-dscp] | user-datagram }

no qos encaps-header dscp-marking { *dscp_code* | copy-from-user-datagram [ignore-pcf-signaled-dscp] }

no

Enables/Disables the **qos encaps-header**.
The value must be expressed as a hexadecimal value from 0x00 through 0x3F.

dscp-marking *dscp_code*

Uses the DSCP code value marked in the IP header of packet/flow to determine the QoS for traffic policing. *dscp_code* must be expressed as a hexadecimal number from 0x00 through 0x3F.

copy-from-user-datagram

Uses the DSCP code value from the user datagram (UDP header) to determine the QoS for traffic policing.

ignore-pcf-signaled-dscp

Overrides the highest priority DSCP value signaled by the PCF.

user-datagram

Uses the DSCP value copied from the user datagram.

Usage

Use this command to apply the QoS policy based on the DSCP value encapsulated in the IP packet header to police subscriber session traffic flows.

Important: For more information on the QoS traffic policing, see the *System Administration Guide*.

Example

The following command sets QoS policy with DSCP code value to *0x0C* for Class 1, silver (AF12):

```
qos encaps-header dscp-marking 0x0c
```

qos traffic-police

Enables and configures Quality of Service (QoS) policy for flow-based traffic policing of subscriber session flows on a per-flow basis.

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

qos traffic-police committed *bps* **peak** *bps* **burst-size** *byte* **exceed-action { drop | lower-ip-precedence | allow } violate-action { drop | lower-ip-precedence | allow }**

no qos traffic-police

---

no

Enables/Disables the **qos traffic-police**

Important: This parameter should be configured to be greater than the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

---

burst-size *bytes*

Default: 3000
Specifies the allowed peak burst size in bytes. *bytes* must be an integer from 0 through 4294967295.

Important: This parameter should be configured to be greater than the following two values: 1) three times greater than the packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

---

committed *bps*

Default: 144000
Specifies the committed data rate (guaranteed-data-rate) in bits per second (bps).
bps must be an integer from 0 through 4294967295.

---

exceed-action { drop | lower-ip-precedence | allow }

Default: **lower-ip-precedence**
Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:
drop: Drops the packet
lower-ip-precedence: Transmits the packet after lowering the ip-precedence
allow: Transmits the packet

---

peak *bps*

Default: 256000

Specifies the peak data-rate for the subscriber in bits per second (bps).
bps must be an integer from 0 through 4294967295.

violate-action { drop | lower-ip-precedence | allow }

Default: drop
Specifies the action to take on the packets that exceed both the committed-data-rate and the peak-data-rate.
The following actions are supported:
drop: Drops the packet
lower-ip-precedence: Transmits the packet after lowering the IP precedence
allow: Transmits the packet

Usage

Use this command to apply the QoS policy to a subscriber session flow for flow-based traffic policing.

Important: For additional information on the QoS traffic policing, see the *System Administration Guide*.

Example

The following command sets the committed data rate to *102400* bps with a peak data rate of *128000* bps and a burst size of *2048* bytes. This lowers the IP precedence when the committed-data-rate is exceeded and drops the packets when the peak-data-rate are violated:

```
qos traffic-police commited 102400 peak 128000 burst-size 2048 exceed-
action lower-ip-precedence violate-action drop
```

qos user-datagram dscp-marking

Enables and configures Quality of Service (QoS) policy related to differentiated service code point (DSCP) marking in the user datagrams of subscriber session flows on a per-flow basis.

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

qos user-datagram dscp-marking *dscp_code*

no qos user-datagram dscp-marking

dscp_code

Specifies the use of the DSCP code value marked in the IP header of packet/flow to determine the QoS for traffic policing. *dscp_code* must be expressed as a hexadecimal number from 0x00 through 0x3F.

Usage

Use this command to apply the QoS policy to subscriber session flow by DSCP marking in user datagram.

Example

The following command sets DSCP marking for user datagram as *0x01* for QoS to subscriber session flow:

```
qos user-datagram dscp-marking 0x01
```

sess-tp-trigger

Configures the trigger for traffic policing based on the traffic volume for a subscriber session.

Product

PDSN, HA, ASN-GW, HSGW, P-GW, SCM

Privilege

Security Administrator, Administrator

Syntax

sess-tp-trigger volume *volume* **direction { both | downlink | uplink }**

no sess-tp-trigger

no

Enables or disables the **sess-tp-trigger**

volume

Specifies the traffic volume threshold (in bytes) that triggers traffic control. *volume* is an integer from 1 through 4294967295.

Usage

Use this command to trigger traffic control based on the traffic volume for a subscriber session. This command requires the purchase and installation of a license.

Example

```
sess-tp-trigger 500
```

type

Specifies the type of traffic policy within a specific Policy-Map.

Product

PDSN, HA, ASN GW, HSGW, P-GW, SCM

Privilege

Administrator

Syntax

type { accounting | dynamic { three-gpp2 rev-A profile-id { any | id *profile_id* **| range** *low_value* **to** *high_value* **} flow-id { any | id** *flow_id* **| range** *low_value* **to** *high_value* **} | pre-provisioned wimax asn-service-profile-id { any | id** *service_id* **} asn-pdfid { any | id** *pdf_id* **} | static | template }**

accounting

Specifies the type of traffic policing as accounting for this specific policy map. This configuration is used for enabling/disabling the accounting of different flows matching conditions within this Policy-Map.

dynamic

Identifies the type of policy map as dynamic.

three-gpp2 rev-A

Configures the dynamic policy map type for CDMA2000-3GPP2 RevA service.

profile-id { any | id *profile_id* **| range** *low_hex* **to** *high_hex* **}**

Specifies the profile id matching within this policy map.
any: allows any profile identifier matching this policy map.
id *profile_id*: allows specific profile identifier matching with in this policy map. *profile_id* must be a hexadecimal number from 0x0 to 0xFFFF.
range *low_value* **to** *high_value*: identifies a range in which a profile identifier must fall within to be considered a match. *low_value* and *high_value* must be either a hexadecimal number from 0x0 to 0xFFFF, or an integer from 0 through 65535 characters.

flow-id { any | id *flow_id* **| range** *low_hex* **to** *high_hex* **}**

Specifies the flow id matching in this policy map.
any allows any flow identifier matching with in this policy map.
id *flow_id* allows specific flow identifier matching with in this policy map. *flow_id* must be either a a hexadecimal number from 0x0 to 0xFFFF, or an integer from 0 to 65535.
range *low_value* **to** *high_value*: identifies a range in which a flow identifier must fall within to be considered a match. *low_value* and *high_value* must be either a hexadecimal number from 0x0 to 0xFFFF, or an integer 0 to 65535.

pre-provisioned

Identifies the type of policy map as pre-provisioned.

wimax

Configures WiMAX service policy map in an ASN-GW service.

asn-service-profile { any | id *service_id* **}**

Specifies the ASN Service profile identifier to match with in this policy map.
any: Allows any ASN Service Profile Identifier matching within this policy map.
id *service_id*: Allows specific Service Profile matching to a specified identifier. *service_id* must be an integer from 1 to 65535 that matches a service ID that was configured in the Subscriber Configuration Mode.

asn-pdfid { any | id *pdf_id* **}**

Specifies the ASN Packet Data Flow Identifier to match with in this policy map.
any: Allows any ASN Packet Data Flow Identifier matching within this policy map.
id *pdf_id*: Allows specific Packet Data Flow matching to a specified identifier. *pdf_id* must be an integer from 1 to 255 that matches a PDF ID that was configured in the Subscriber Configuration Mode.

static

Specifies the type of traffic policing as static for this specific Policy Map. In this type of policy, the traffic flow classification and flow treatment is pre-defined with classification rules through Class-Map configuration.
This is the detailed type of policy map.

template

Specifies the type of traffic policy to as a template to all subscribers associated with this policy map.

Usage

Specifies the type of traffic policy within the specific Policy-Map.

Example

The following commands configures the traffic policy for this Policy-Map as static:

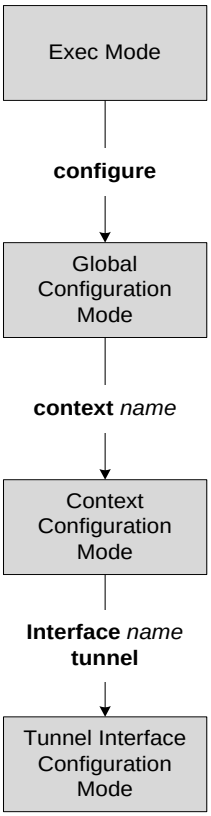
```
type static
```

The following commands configures the traffic policy for this Policy-Map as pre-provisioned for WiMAX service requiring a match of any service profile and PDF id of *3*:

```
type pre-provisioned wimax asn-service-profile any asn-pdfid id 3
```

Chapter 267
Tunnel Interface Configuration Mode Commands

The Tunnel Interface Configuration Mode is used to create and manage the IP interfaces for various types of tunnels including associated parameters, such as addresses and address resolution options.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

description

Enters descriptive text for the current interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

description *text*

no description

no

Clears the description for the interface.

text

Contains the descriptive text for this interface. *text* must be an alphanumeric string of 0 through 79 characters. If spaces are required, the string must be bracketed with double quotation marks (“). The interface description is case sensitive.

Usage

Set the description to provide useful information regarding the interface’s primary function, services, end users, etc.

Example

The following command describes this interface:

```
description sampleInterfaceDescriptiveText
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

ip address

Configures the IPv4 address for this tunnel interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ip address [*ip_address***/***ip_mask* **|** *ip_address ip_mask***]**

no ip address *ip_address*

no

Removes the configured IPv4 address bound to a tunnel interface.

*ip_address***/***ip_mask* **|** *ip_address ip_mask*

Specifies a destination IP address or group of addresses that will use this route.
*ip_address***/***ip_mask*: Specifies a combined IP address subnet mask bits to indicate what IP addresses to which the route applies. *ip_address***/***ip_mask* must be specified using IPv4 dotted-decimal and CIDR notation. *ip_mask*is an integer which is the number of bits in the subnet mask.
ip_address ip_mask: Specifies an IP address and the networking (subnet) mask pair which is used to identify the set of IP addresses to which the route applies. *ip_address* must be specified using the IPv4 dotted-decimal notation. *ip_mask* must be specified using the IPv4 dotted-decimal notation as network mask for subnets.
The mask as specified by *ip_mask* or resulting from *ip_address***/***ip_mask* is used to determine the network for packet routing.
Zeroes ("0") in the resulting mask indicate that the corresponding bit in the IP address is not significant in determining the network for packet routing.
Ones ("1") in the resulting mask indicate the corresponding bit in the IP address is significant in determining the network.

Usage

Use this command to bind the IPv4 address to a tunnel interface. This address does not affect the encapsulation of packets going out on the tunnel interface.

Example

The following command will assign the *10.2.3.4* as IPv4 address to this tunnel interface:

```
ip address 10.2.3.4
```

ipv6 address

Configures the IPv6 address for the specific tunnel interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax

ipv6 address *ipv6_address/ipv6_mask*

no ipv6 address *ipv6_address*

no

Removes the configured IPv6 address bound to a tunnel interface.

*ipv6_address***/***ipv6_mask*

Specifies a destination IP address or group of addresses that will use this route.
*ipv6_address***/***ipv6_mask*: Specifies a combined IP address subnet mask bits to indicate what IP addresses to which the route applies. *ipv6_address***/***ipv6_mask* must be specified usingIPv6 colon-separated and CIDR notation. *ipv6_mask* is a numeric value which is the number of bits in the subnet mask.

Usage

Use this command to bind the IPv6 address to a tunnel interface. This address does not affect the encapsulation of packets going out on the tunnel interface.

Example

The following command will assign the *1001::2:010:1234* as IPv6 address to this tunnel interface:

```
ipv6 address 1001::2:010:1234
```

tunnel-mode

Configures the tunnel mode type for this tunnel interface. It also enters the specific tunnel configuration mode, if required.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
tunnel-mode { gre | ipv6ip }

defualt tunnel-mode
```

default

Sets the default tunnel mode for this interface. By default, the tunnel mode is set to IPv6-to-IPv4 type.

gre

Default: Disabled
Sets the tunnel interface mode to Generic Routing Encapsulation (GRE) type and enters the GRE Tunnel Configuration mode, if required.

ipv6ip

Default: Enabled
Sets the tunnel interface mode to IPv6-to-IPv4 type and creates the IPv6-to-IPv4 Tunnel Configuration mode, if required.

Usage

Use this command to set the tunnel mode type of GRE or IPv6-to-IPv4 for the tunneling interface.

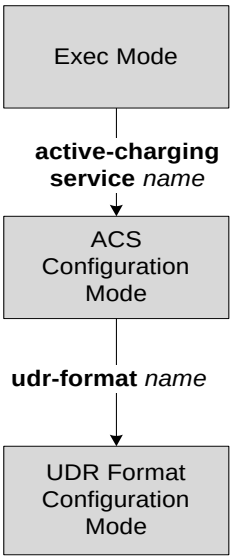
Example

The following command sets the tunnel mode to GRE for specific interface:

```
tunnel-mode gre
```

Chapter 268
UDR Format Configuration Mode Commands

The UDR Format Configuration Mode enables configuring User Detail Record (UDR) formats.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

attribute

This command allows you to specify the fields and their order in UDRs.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
attribute attribute { [ format { MM/DD/YY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-
HH:MM:SS | YYYYMMDDHHMMSS | seconds } [ localtime ] | [ { bytes | pkts } { downlink |
uplink } ] ] priority priority }

no attribute attribute [ priority priority ]
```

no

If added previously, removes the specified attribute from the UDR format.

attribute *attribute*

Specifies the attribute.
attribute must be one of the following:

Attribute	Description
diameter-session-id	This attribute reports Diameter session identifier. ***Important:*** This attribute is customer specific, and is only available in 8.3 and later releases.
failure-handling-mode	This attribute reports failure handling mode in case the Online Charging System (OCS) goes abnormal.
radius-called-station-id	This attribute reports the Called Station ID of the mobile handling the flow.
radius-calling-station-id	This attribute reports the Calling Station ID of the mobile handling the flow.
radius-fa-nas-identifier	This attribute reports the RADIUS NAS identifier of Foreign Agent (FA).
radius-fa-nas-ip-address	This attribute reports the RADIUS IP address of Foreign Agent (FA).
radius-nas-identifier	This attribute reports the RADIUS NAS identifier.
radius-nas-ip-address	This attribute reports the RADIUS NAS IP address. Note that this attribute is interchangeable with **sn-st16-ip-addr** for the user.
radius-user-name	This attribute reports the user name associated with the flow.

Attribute	Description
sn-3gpp2-bsid	This option has been deprecated. To configure this attribute see the rule-variable command.
sn-3gpp2-carrier-id	This option has been deprecated. To configure this attribute see the rule-variable command.
sn-3gpp2-esn	This option has been deprecated. To configure this attribute see the rule-variable command.
sn-3gpp2-meid	This option has been deprecated. To configure this attribute see the rule-variable command.
sn-3gpp2-service-option	This option has been deprecated. To configure this attribute see the rule-variable command.
sn-acct-beginning-session	This attribute reports the Session Beginning information. ***Important:*** This attribute is customer specific, and is only available in 8.3 and later releases.
sn-acct-session-continue	This attribute reports the Session Continue information. ***Important:*** This attribute is customer specific, and is only available in 8.3 and later releases.
sn-acct-session-id	This attribute reports the Accounting Session identifier.
sn-acct-session-time	This attribute reports the duration from acct-status-type:start to acct-status-type:stop. ***Important:*** This attribute is customer specific, and is only available in 8.3 and later releases.
sn-acct-status-type	This attribute reports the Accounting Status identifier. ***Important:*** This attribute is customer specific, and is only available in 8.3 and later releases.
sn-charging-type	This attribute reports the charging type: offline or online. ***Important:*** This attribute is customer specific, and is only available in 8.3 and later releases.

Attribute	Description
sn-closure-reason	This attribute reports the reason for termination of the flow/UDR: • 0 = CALL_TERMINATION — normal, such as subscriber session ended • 1 = PDSN_HO — handoff control processing specified • 2 = TIME_LIMIT • 3 = VOLUME_LIMIT • 4 = MGMT_INTERVENTION • 5 = ACCT_SESS_START • 6 = CCRU_RESPONSE • 7 = OFFLINE_CHARGING — for UDRs generated when offline charging trigger is received from DCCA
sn-content-id	This attribute reports the unique identifier for the content-id.
sn-content-label	This attribute reports the identifier for text label for content-id.
sn-content-vol	This attribute reports the identifier for content volume.
sn-correlation-id	This attribute reports the RADIUS correlation identifier.
sn-duration	This attribute reports the time difference between the first and last packet of a single data flow accounted in the UDR record. For example, the time difference between the first ICMP echo request and the last ICMP echo response before the record gets written for the content-id.
sn-end-time [format *format*]	This attribute reports the timestamp for last packet of flow in UTC.
sn-fa-correlation-id	This attribute reports the RADIUS Correlation Identifier of the Foreign Agent (FA).
sn-fa-ip-address	This attribute reports IP address of the FA.
sn-filler-blank	This attribute inserts a blank filler field, generates an empty UDR field.
sn-filler-zero	This attribute inserts a “0” in the UDR field.
sn-format-name	This attribute reports name of the UDR format used.
sn-group-id	This attribute reports the sequence group identifier for the records.
sn-ha-ip-address	This attribute reports IP address of the Home Agent (HA). ***Important:*** This attribute is customer specific, and is only available in 8.3 and later releases.
sn-local-seq-no	This attribute reports unique local sequence number of UDR identifier per ACSMgr/SessMgr and linearly increasing in UDR file.

Attribute	Description
sn-ocs-ip-address	This attribute reports IP address of the Online Charging Server. ***Important:*** This attribute is customer specific, and is only available in 8.3 and later releases.
sn-rulebase	This attribute reports name of the ACS rulebase used.
sn-sequence-no	This attribute reports unique sequence number (per **sn-sequence-group** and **radius-nas-ip-address**) of UDR identifier and linearly increasing in UDR file.
sn-served-bsa-addr	This attribute reports address of Base Station Area being served.
sn-service-name	This attribute reports name of the ACS service.
sn-st16-ip-addr	This option has been deprecated. This attribute reports IP address of the chassis handling this flow. This attribute is interchangeable with **radius-nas-ip-address** for other systems.
sn-start-time [format *format* **]**	This attribute reports timestamp for first packet of flow in UTC.
sn-stream-number	This attribute reports unique UDR billing record identifier. ***Important:*** This attribute is customer specific, and is only available in 8.3 and later releases.
sn-subscriber-id	This attribute reports subscriber ID.
sn-subscriber-nat-flow-ip	This attribute reports NAT IP address(es) of NAT-enabled subscriber.
sn-timestamp	This attribute reports timestamp when the UDR is actually generated. ***Important:*** This attribute is customer specific, and is only available in 8.3 and later releases.

format { MM/DD/YY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds }

Specifies the timestamp format.

localtime

Specifies the local time. By default, timestamps are displayed in Coordinated Universal Time (UTC).

{ bytes | pkts } { downlink | uplink }

Specifies bytes/packets sent/received from/by mobile.

priority *priority*

Specifies the position priority of the field within the UDR. Lower numbered priorities (across all attribute, event-label, and rule-variable) occur first.
priority must be an integer from 1 through 65535. Up to 50 position priorities (across all attribute, event-label, and rule-variable) can be configured.

Usage

Use this command to set the attributes and priority for UDR file format.
A particular field in UDR format can be entered multiple times at different priorities. While removing the UDR field using the **no attribute** command, you can either remove all occurrences of a particular field by specifying the field name or remove a single occurrence by additionally specifying the optional **priority** keyword.
Consider the following scenario. If the volume/time threshold interval is large enough (or disabled). At time t=0, 10 ICMP packets are sent, which takes 9 seconds. There is nothing for the next 100 seconds, and then again 10 ICMP packets are sent which takes 10 seconds, and then again nothing for next the 60 seconds and then the session is terminated.
In this scenario:

- sn-start-time should be t = 0.
- sn-end-time should be t = 0+9+100+10 (sn-end-time would be the last ICMP packet sent).
- sn-duration should be sn-end-time minus sn-start-time, i.e. 0+9+100+10 – 0 = 119 seconds (since the ICMP flow would exist between the two intervals of sending ICMP packets, the sn-start-time would be that of the first packet of the flow and sn-end-time of the last packet (20th packet). Hence, sn-duration would take into account all the seconds between the first and last packet of the flow).

Example

The following is an example of this command:

```
attribute radius-user-name priority 12
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

event-label

This command allows you to specify an optional event label/identifier to be used as an attribute in the UDRs.

Product

All

Privilege

Security Administrator, Administrator

Syntax

event-label *event_label* **priority** *priority*

no event-label

no

If previously configured, removes the event label configuration.

event_label

Specifies the event label/identifier to be used as UDR attribute.
event_label must be an alphanumeric string of 1 through 63 characters.

priority *priority*

Specifies the Comma Separated Value (CSV) position of the attribute (label/identifier) in the UDR.
priority must be an integer from 1 through 65535.

Usage

Use this command to configure an optional event label/identifier as an attribute in the UDR and its position in the UDR.

Example

The following is an example of this command:

```
event-label radius_csv1 priority 23
```

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

rule-variable

This command allows you to specify fields and their order in UDRs.

Product

All

Privilege

Security Administrator, Administrator

Syntax

rule-variable *rule_variable* **priority** *priority*

no rule-variable *rule_variable* **[priority** *priority* **]**

no

If previously configured, removes the specified rule variable configuration.

rule-variable *rule_variable*

Specifies the rule variable for the UDR format.
rule_variable must be one of the following options:

- **bearer 3gpp2**: Bearer-related configuration:
  - **always-on**
  - **bsid**
  - **carrier-id**
  - **esn**
  - **ip-qos**
  - **ip-technology**
  - **meid**
  - **release-indicator**
  - **serv-MDN**
  - **service-option**
  - **session-begin**
  - **session-continue**

Important: For more information on protocol-based rules see the *ACS Ruledef Configuration Mode Commands* chapter.

priority *priority*

Specifies the CSV position of the field (protocol rule) in the UDR.
priority must be an integer from 1 through 65535.

Usage

Use this command to specify what field appears in which order in the UDR.
A particular field in UDR format can be entered multiple times at different priorities. While removing the UDR field using the **no rule-variable** command, you can either remove all occurrences of a particular field by specifying the field name, or remove a single occurrence by additionally specifying the optional priority keyword.

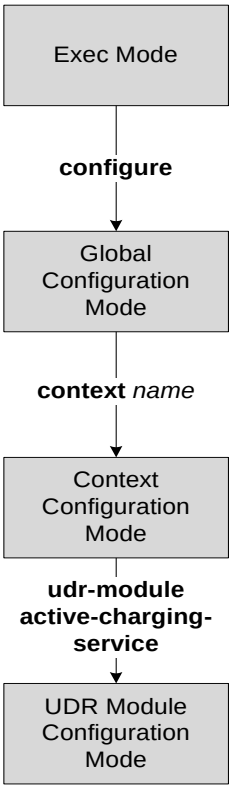
Example

The following is an example of this command:

```
rule-variable bearer 3gpp2 bsid priority 36
```

Chapter 269
UDR Module Configuration Mode Commands

The UDR Module Configuration Mode allows you to configure Usage Data Record (UDR) file transfer parameters.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

cdr

This command allows you to configure EDR/UDR file transfer parameters.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
cdr { purge { storage-limit storage_limit | time-limit time_limit } [ max-files
max_records_to_purge ] | push-interval push_interval | push-trigger space-usage-percent
trigger_percentage | remove-file-after-transfer | transfer-mode { pull [ module-only ] |
push primary { encrypted-url encrypted_url | url url } [ [ max-files max_records ] [
module-only ] [ secondary { encrypted-secondary-url encrypted_secondary_url | secondary-
url secondary_url } ] [ via local-context ] + ] | use-harddisk }

default cdr [ purge | push-interval | push-trigger space-usage-percent | remove-file-
after-transfer | transfer-mode [ module-only | push via ] | use-harddisk ] +

no cdr [ purge | remove-file-after-transfer | use-harddisk ] +
```

default

Configures the default setting for the specified keyword(s):

- **purge**: Disabled
- **push-interval**: 300 seconds
- **push-trigger**: 80 percent
- **remove-file-after-transfer**: Disabled
- **transfer mode**: Pull
- **push via**: line card is used for push
- **use-harddisk**: Disabled

Important: The **use-harddisk** keyword is only available on ASR 5000 chassis.

no

If previously configured, disables the specified configuration:

- **purge**: Disables purging of records.
- **remove-file-after-transfer**: Retains a copy of the file even after it has been pushed or pulled to another server.
- **use-harddisk**: Disables data storage on the SMC hard disk.

Important: The **use-harddisk** keyword is available only on the ASR 5000 chassis.

purge { storage-limit *storage_limit* **| time-limit** *time_limit* **} [max-files** *max_records_to_purge* **]**

Specifies to purge/delete the CDR/UDR records based on "time" or "volume" limit.

- **storage-limit** *storage_limit*: Specifies to start deleting files when the specified megabytes of space is used for storage.

  storage_limit specifies the volume limit for the record files, in megabytes, and must be an integer from 10 through 143360.

- **time-limit** *time_limit*: Specifies to start deleting files older than the specified time limit.

  time_limit specifies the time limit for the record files, and must be an integer from 600 through 2592000.

- **max-files** *max_records_to_purge*: Specifies the maximum number of records to purge.

  max_records_to_purge must be an integer from 1000 through 10000.

push-interval *value*

Specifies the transfer interval (in seconds) to push UDR/EDR files to an external file server.
value must be an integer from 60 through 3600.
Default: 300

push-trigger space-usage-percent *trigger_percentage*

Specifies the UDR/EDR disk space utilization percentage, upon reaching which an automatic push is triggered and files are transferred to the configured external server.
trigger_percentage specifies the UDR/EDR disk utilization percentage for triggering push, and must be an integer from 10 through 80.
Default: 80%

remove-file-after-transfer

Specifies that the system must delete UDR/EDR files after they are transferred to the external file server.
Default: Disabled

transfer-mode { pull [module-only] | push primary { encrypted-url *encrypted_url* **| url** *url* **} [[max-files** *max_records* **] [module-only] [secondary { encrypted-secondary-url** *encrypted_secondary_url* **| secondary-url** *secondary_url* **}] [via local-context] +]**

Specifies the UDR/EDR file transfer mode.

- **pull**: Specifies that the L-ESS is to pull the CDR files.
- **push**: Specifies that the system is to push CDR files to the configured L-ESS.
- **max-files** *max_records*: Specifies the maximum number of files sent per iteration based on configured file size.

  Default: 4000

- **module-only**: Specifies that the transfer-mode is only applicable to the UDR module; if not configured it is applicable to both EDR and UDR modules. This enables support for individual record transfer-mode configuration for each module.
- **primary encrypted-url** *encrypted_url*: Specifies the primary location in encrypted format to which the system pushes the CDR files.

encrypted_url must be the primary location name in an encrypted format, and must be an alphanumeric string of 1 through 1024 characters.

- **primary url** *url*: Specifies the primary location to which the system pushes the CDR files.

  url must be the primary location, and must be an alphanumeric string of 1 through 1024 characters in the format: *//user:password@host:[port]/directory*.

- **secondary encrypted-secondary-url** *encrypted_secondary_url*: Specifies the secondary location in encrypted format to which the system pushes the CDR files when the primary location is unreachable or fails.

  encrypted_secondary_url must be the location in an encrypted format, and must be an alphanumeric string of 1 through 1024 characters.

- **secondary secondary-url** *secondary_url*: Specifies the secondary location to which the system pushes the CDR files when the primary location is unreachable or fails.

  secondary_url must be the secondary location, and must be an alphanumeric string of 1 through 1024 characters in the format: *//user:password@host:[port]/directory*.

- **via local-context**: Selects the LC/SPIO for transfer of CDRs. The system pushes the UDR files via SPIO in the local context.

use-harddisk

Important: The **use-harddisk** keyword is available only on the ASR 5000 chassis.

Specifies that on an ASR 5000 chassis, the hard disk on the SMC will be used to store UDR/EDR files. When configured to use the hard disk for UDR/EDR storage, UDR/EDR files are transferred from packet processing cards to the hard disk on the SMC.
Default: Disabled

+

Indicates that more than one of the previous keywords can be entered within a single command.

Usage

Use this command to configure how charging data records (CDR) are moved and stored.
On the ASR 5000 chassis, run this command only from the local context. Running in any other context would fail and deliver an error message.
If PUSH transfer mode is configured, the L-ESS server URL to which the CDR files need to be transferred to must be specified. The configuration allows a primary and a secondary server to be configured. Configuring the secondary server is optional. Whenever a file transfer to the primary server fails for four consecutive times, the files will be transferred to the secondary server. The transfer will switch back to the original primary server when:

- Four consecutive transfer failures to the secondary server occur
- After switching from the primary server, 30 minutes elapses

When changing the transfer-mode from pull to push, disable the PULL from L-ESS and then change the transfer mode to push. Make sure that the push server URL configured is accessible from the local context. Also, make sure that the base directory that is mentioned contains udr directory created within it.
When changing the transfer-mode from push to pull, after changing, enable PULL on the L-ESS. Any of the ongoing PUSH activity will continue till all the scheduled file transfers are completed. If there is no PUSH

activity going on at the time of this configuration change, all the PUSH related configuration is nullified immediately.

The **cdr use-harddisk** command is available only on the ASR 5000 chassis. This command can be run only in a context where CDRMOD is running. Configuring in any other context will result in failure with the message *"Failure: Please Check if CDRMOD is running in this context or not."*

The **cdr use-harddisk** command can be configured either in the UDR or EDR module, but will be applicable to both record types. Configuring in one of the modules will prevent the configuration to be applied in the other module. Any change to this configuration must be done in the module in which it was configured, the change will be applied to both record types.

The VPNMgr can send a maximum of 4000 files to the remote server per iteration. However if the individual file size is big (say when compression is not enabled), then while transferring 4000 files SFTP operation takes a lot of time. To prevent this, the **cdr transfer-mode push** command can be configured with the keyword **max-files**, which allows operators to configure the maximum number of files sent per iteration based on configured file size.

Example

The following command configures the system to retain a copy of the data file after it has been transferred to the storage location:

```
no cdr remove-file-after-transfer
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

file

This command allows you to configure UDR file parameters.

Product

All

Privilege

Security Administrator, Administrator

Syntax

file [charging-service-name { include | omit }] [compression { gzip | none }] [current-prefix *string* **] [delete-timeout** *seconds* **] [directory** *directory_name* **] [exclude-checksum-record] [field-separator { hyphen | omit | underscore }] [file-sequence-number rulebase-seq-num] [headers] [name** *file_name* **] [reset-indicator] [rotation [num-records** *number* **| time** *seconds* **| volume** *bytes* **]] [sequence-number { length** *length* **| omit | padded | padded-six-length | unpadded }] [storage-limit** *limit* **] [time-stamp { expanded-format | rotated-format | unix-format }] [trailing-text** *string* **] [trap-on-file-delete] [udr-seq-num] [xor-final-record] +**

default file [charging-service-name] [compression] [current-prefix] [delete-timeout] [directory] [field-separator] [file-sequence-number] [headers] [name] [reset-indicator] [rotation { num-records | time | volume }] [sequence-number] [storage-limit] [time-stamp] [trailing-text] [udr-seq-num]

---

default

Configures the default setting for the specified keyword(s). Using the **default file** command will reset some but not all keyword parameters to their default values. To ensure that the default is reset for a specific parameter, include the corresponding keyword in the command.

---

charging-service-name { include | omit }

Specifies to include/exclude name of the charging service in the file name.

- **include**: Includes name of the charging service in the UDR file name.
- **omit**: Excludes name of the charging service in the UDR file name.

Default: **include**

---

compression { gzip | none }

Configures gzip compression of the UDR file.

- **gzip**: Enables GNU zip compression of the UDR file at approximately 10:1 ratio.
- **none**: Disables Gzip compression.

Default: **none**

---

current-prefix *string*

Specifies a string to add to the beginning of the UDR file that is currently being used to store UDR records. *string* must be an alphanumeric string of 1 through 31 characters.
Default: curr

delete-timeout *seconds*

Specifies a timeout period (in seconds) when completed UDR files are deleted. By default, files are never deleted.
seconds must be an integer from 3600 through 31536000.
Default: Disabled

directory *directory_name*

Specifies a subdirectory in the default directory in which to store UDR files.
directory_name must be an alphanumeric string of 1 through 191 characters.
Default: /records/udr

exclude-checksum-record

When entered, this keyword excludes the final record containing #CHECKSUM followed by the 32-bit Cyclic Redundancy Check (CRC) of all preceding records from the UDR file.
Default: Disabled, inserts checksum record into the UDR file header.

field-separator { hyphen | omit | underscore }

Specifies the field separators to be used between two fields of a UDR file name.

- **hyphen**: Specifies to use '-' (hyphen) as the field separator.
- **omit**: Excludes the field separator.
- **underscore**: Specifies to use '_' (underscore) as the field separator.

Default: **underscore**

file-sequence-number rulebase-seq-num

Generates unique file sequence numbers for different rulebase-format-name combinations.

headers

Includes a file header summarizing the record layout.

name *file_name*

Default: udr
Specifies a string to use as the base file name for UDR files.
file_name must be an alphanumeric string of 1 through 31 characters. The file name format is as follows:
base_rulebase_format_sequencenum_timestamp

- *base*: Specifies type of record in file or contains the operator-specified string. Default: udr
- *rulebase*: Specifies the name of the ACS rulebase. UDRs from different rulebases go into different UDR files.
- *format*: Specifies the name of the UDR format if **single-udr-format** is specified, else the format field (and the trailing underscore) is omitted from the file name.
- *sequencenum*: This is a 5-digit sequence number to detect the missing file sequence. It is unique among all UDR files on the system.
- *timestamp*: Contains a timestamp based on file creation time in UTC formatted as: MMDDYYYYHHMMSS.

UDR files that have not been closed have a string added to the beginning of their file names.

File name for a UDR file in CSV format that contains information for a rulebase named *rulebase1* and a UDR schema named *udr_schema1* appears as follows:
udr_rulebase1_udr_schema1_00005_01302006143409
If file name is not configured, the system creates files for EDRs/UDRs/FDRs (xDRs) using the following name template with limits to 256 characters:
basename_ChargSvcName_ timestamp_SeqNumResetIndicator_FileSeqNumber

- *basename*: A global-based configurable text string that is unique per system that uniquely identifies the global location of the system running ACS.
- *ChargSvcName*: A system context-based configurable text string that uniquely identifies a specific context-based charging service.
- *timestamp*: Date and time at the instance of file creation. Date and time in the format: "MMDDYYYYHHmmSS", where HH is a 24-hour value from 00-23.
- *SeqNumResetIndicator*: A one-byte counter used to discern the potential for duplicated FileSeqNumber with a range of 0 through 255, which is incremented by a value of 1 for the following conditions:
  - Failure of an ACS software process on an individual packet processing card
  - Failure of the system such that a second system takes over (for example, a standby or backup chassis put in place according to Inter-chassis Session Recovery)
  - File Sequence Number (FileSeqNumber) rollover from 999999999 to 0
- *FileSeqNumber*: unique file sequence number for the file is a 9-digit integer from 000000000 through 999999999. It is unique on each chassis.

File name for a closed xDR file in CSV format that contains information for ACS *xyz_city1* and charging service name *preapaid2* with timestamp *12311969190000*, and file sequence number counter reset indicator to *002* for file sequence number *034939002* appears as follows:
xyz_city1_preapaid2_12311969190000_002_034939002
File name for a running xDR file in CSV format that contains information for the same parameters for file sequence number *034939003* prefixed with *curr_* and appears as follows:
curr_xyz_city1_preapaid2_12311969190000_002_034939002

---

reset-indicator

Specifies to include the reset indicator counter value, from 0 to 255, in the UDR file name and is incremented (by one) whenever any of the following conditions occur:

- An ACSMgr/SessMgr process fails.
- An Inter-chassis Session Recovery (ICSR) peer chassis has transitioned from standby to active.
- The sequence number in sequence-number keyword has rolled over to zero.

---

rotation { num-records *records* **| time** *seconds* **| volume** *bytes* **}**

Specifies when to close a UDR file and create a new one.

- **num-records** *records*: Specifies the number of records that should be added to the file. When the number of records in the file reaches this specified value, the file is complete.

  records must be an integer from 100 through 10240.

  Default: 1024

- **time** *seconds*: Specifies the period of time to wait before closing the UDR file and creating a new one.

  seconds must be an integer from 30 through 86400.

Default: 3600 seconds

- **volume** *bytes*: Specifies the maximum size of the UDR file before closing it and creating a new one.

  bytes must be an integer from 51200 through 62914560.

  Default: 102400 bytes

  Note that higher settings may provide the best compression ratio when the **compression** keyword is set to *gzip*.

---

sequence-number { length *length* **| omit | padded | padded-six-length | unpadded }**

Specifies including or excluding the sequence number in the file name.

- **length** *length*: Includes the sequence number with the specified length.

  length must be the length of the file sequence number with preceding zeroes in the file name, and must be an integer from 1 through 9.

  Important: The **length** configuration is applicable in both UDR and EDR modules. When applied in both modules without the **file udr-seq-num** configuration, the minimum among the two values will come into effect for both modules. With the **file udr-seq-num** config, each module will use its own value of length.

- **omit**: Excludes the sequence number from the file name.
- **padded**: Includes the padded sequence number with preceding zeros in the file name. This is the default setting.
- **padded-six-length**: Includes the padded sequence number with six preceding zeros in the file name.
- **unpadded**: Includes the unpadded sequence number in the file name.

Default: **padded**

---

storage-limit *limit*

Specifies deleting files when the specified amount of space, in bytes, is used up for UDR/EDR file storage on packet processing card RAM.
On an ASR 5000 chassis, *limit* must be an integer from 10485760 through 536870912.
Default: 33554432

Important: On the ASR 5000 chassis, the total storage limit is 536870912 bytes (512 MB). This limit is for both UDR and EDR files combined.

---

time-stamp { expanded-format | rotated-format | unix-format }

Specifies the timestamp of when the file was created be included in the file name.

- **expanded-format**: Specifies the UTC MMDDYYYYHHMMSS format.
- **rotated-format**: Specifies the YYYYMMDDHHMMSS format.
- **unix-format**: Specifies the UNIX format of *x.y*, where *x* is the number of seconds since 1/1/1970 and *y* is the fractional portion of the current second that has elapsed.

---

trailing-text *string*

Specifies the inclusion of arbitrary text string in the file name.

string must be an alphanumeric string of 1 through 30 characters.

trap-on-file-delete

Instructs the system to send an SNMP notification (trap) when an UDR/EDR file is deleted due to lack of space.
Default: Disabled

udr-seq-num

Specifies that the file sequence numbers that are part of the UDR file names be independently generated. If disabled, a single set of sequence numbers are shared by both UDR and EDR files.
Default: Disabled

xor-final-record

Specifies inserting an XOR checksum (in place of the CRC checksum) into the UDR file header if the **exclude-checksum-record** keyword is left at its default setting.
Default: Disabled

+

More than one of the previous keywords can be entered within a single command.

Usage

Use this command to configure UDR file characteristics.

Example

The following command sets the prefix of the current active UDR file to *current*:

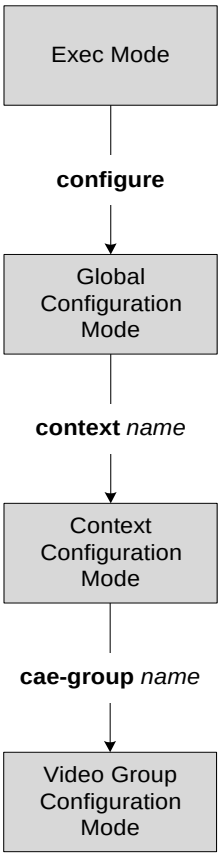
```
file current-prefix current
```

The following command sets the base file name to *UDRfile*:

```
file name UDRfile
```

Chapter 270
Video Group Configuration Mode

The Video Group Configuration Mode is used to add CAEs to a CAE group and configure the CAEs for load balancing and health-check monitoring. The CAE (Content Adaptation Engine) is an optional component of the Mobile Videoscape. For additional information, refer to the *Mobile Video Gateway Administration Guide*.



Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.

keepalive-server

Specifies keep-alive messaging information for Content Adaptation Engine (CAE) health-check monitoring, which is part of CAE load balancing on the Mobile Video Gateway. Note that this command and its options configure settings that apply to all CAEs in the CAE group, not to an individual CAE.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

[default] keepalive-server deadtime *seconds* **interval** *seconds* **num-retry** *num-retries* **port** *port_number* **timeout** *seconds* **[-noconfirm]**

default keepalive-server

Sets the CAE keep-alive settings to their default values.

keepalive-server deadtime *seconds* **interval** *seconds* **num-retry** *num-retries* **port** *port_number* **timeout** *seconds* **[-noconfirm]**

Specifies keep-alive messaging information for CAE health-check monitoring.

deadtime *seconds*

Specifies the periodic retry interval (in seconds) after a CAE is detected down. *seconds* is an integer from 1 through 1800. The default value is 120 seconds.

interval *seconds*

Specifies the interval (in seconds) for how often the Mobile Video Gateway sends a keep-alive message to the CAEs. *seconds* is an integer from 0 through 120. The default value is 10 seconds. A value of 0 turns off keep-alive detection and marks the state of all CAEs to Up.

num-retry *num_retries*

Specifies the number of keepalive retries after a CAE does not respond. *num_retries* is an integer from 1 through 20. The default value is 3 retries.

port *port_number*

Specifies the TCP port number for health-check monitoring, which is an integer from 1 through 65535. The default value is 5100.

timeout *seconds*

Specifies the keep-alive timeout (in seconds) which is an integer from 1 through 30. The default value is 3 seconds.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to specify keep-alive messaging information for CAE health-check monitoring, which is part of CAE load balancing on the Mobile Video Gateway.

Example

The following command specifies keep-alive messaging information for the CAEs in the CAE group:

```
keepalive-server deadtime 120 interval 10 num-retry 3 port 5100 timeout 3
```

local-address

Specifies the local IPv4 address on the Mobile Video Gateway for the keepalive TCP connection used for Content Adaptation Engine (CAE) load balancing.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

[no] local-address *IPv4_address* **[-noconfirm]**

no local-address *IPv4_address*

Deletes the local IPv4 address if previously specified.

local-address *IPv4_address*

Specifies the local IPv4 address on the Mobile Video Gateway for the keep-live TCP connection used for CAE load balancing. *IPv4_address* must be in dotted decimal notation.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to specify the local IPv4 address on the Mobile Video Gateway, in dotted-decimal notation.

Example

The following command specifies the local IPv4 address on the Mobile Video Gateway:

```
local-address 10.2.3.4
```

server

Adds a CAE (Content Adaptation Engine) and its IPv4 address and port number to the associated CAE group. The Mobile Video Gateway uses this information for CAE load balancing. The Mobile Video Gateway has a system limit of 64 CAEs.

Product

MVG

Privilege

Security Administrator, Administrator

Syntax

[no] server *cae_name* **address** *IPv4_address* **port** *port_number* **[-noconfirm]**

no server *cae_name*

Deletes the CAE from the CAE group if previously configured.

server *cae_name* **address** *IPv4_address* **port** *port_number*

Adds a CAE and its IPv4 address and port number to the associated CAE group. *cae_name* is an alphanumeric string of 1 through 15 characters. *IPv4_address* must be in dotted-decimal notation. *port_number* is an integer from 1 through 5535. The default value is 80.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to add a CAE and its IPv4 address and port number to the associated CAE group.

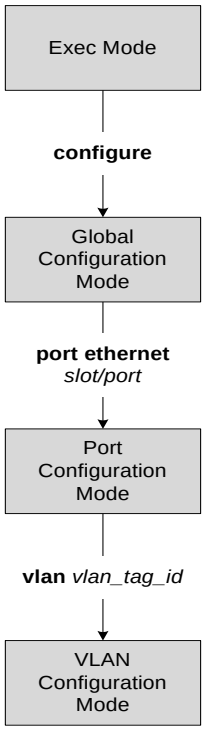
Example

The following command adds a CAE named *cae_1* and its IPv4 address and port number to the associated CAE group:

```
server cae_1 address 10.2.3.4 port 80
```

Chapter 271
VLAN Configuration Mode Commands

The VLAN Configuration Mode is used to create and manage Virtual LANs and their bindings between contexts.



bind interface

Configures a virtual interface to context association for the current VLAN.

Product

HA, HSGW, PDSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

[no] bind interface *interface_name context_name*

no

Indicates the binding between the virtual interface specified and the context specified is to be unbound for the current VLAN.

interface_name context_name

Specifies the name and context of the virtual interface to be bound to the context. *interface_name* must be an alphanumeric string of 1 through 79 characters.
context_name must refer to a previously configured context expressed as an alphanumeric string of 1 through 79 characters.

Usage

Bind a virtual interface and context to allow the VLAN to provide service.

Example

bind interface *sampleVirtual sampleContext*

no bind interface *sampleVirtual sampleContext*

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
end
```

Usage

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.

ingress-mode

Toggles between enabling and disabling the port ingress (incoming) mode.

Product

HA, HSGW, PDSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] ingress-mode
```

no

Disables the port ingress mode.

Usage

Use this command to enable or disable the ingress mode for the port.

Example

```
ingress-mode
```

priority

Configures 802.1p VLAN priority bit for ASN-GW only.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Syntax

priority *value*

no priority

no

Disables the setting of the 802.1p priority bit.

value

Sets the value of the 802.1p priority bit as an integer from 0 through 7, with 7 being the highest priority.

Usage

Set a value for the VLAN priority bit as used in the ANS-GW.
Refer to the *ASN-GW Administration Guide* for additional information on support for 802.1p.

Example

To set a VLAN priority bit value, use the following command:

```
priority 3
```

To disable the use of a VLAN priority bit, use the following command:

```
no priority
```

shutdown

Disables or enables traffic over the current VLAN.

Product

HA, HSGW, PDSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ no ] shutdown
```

no

Enables the VLAN. When omitted the VLAN is shutdown.

Usage

Shut down a VLAN.
To bring a VLAN into service, execute this command using the **no** keyword.

Example

To disable a VLAN from sending or receiving network traffic use the following command:

```
shutdown
```

To enable a VLAN use the following command:

```
no shutdown
```

vlan-map

Sets a single next-hop IP address so that multiple VLANs can use a single next-hop gateway. **vlan-map** is associated with a specific interface.

Product

HA, HSGW, PDSN, P-GW, SGSN

Privilege

Security Administrator, Administrator

Syntax

vlan-map next-hop *ip_address*

next-hop *ip_address*

Defines an IP address for the next-hop gateway.
ip_address: can be entered using IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage

Use **vlan-map** to combine multiple VLAN links to go through a single IP address. This feature is used in conjunction with nexthop forwarding and overlapping IP pools.
After configuring the vlan-map, go to the Port Ethernet Configuration mode to attach the vlan-map to a specific VLAN.

Example

The following command sets an IPv4 for a next-hop gateway.

```
vlan-map next-hop 123.123.123.1
```